



LETTER OF APPOINTMENT

MEMORANDUM FOR IBRAHIIM KENT, FEDSIM PM

Subject: Appointment as Contracting Officer's Representative

You are hereby appointed as the Contracting Officer's Representative (COR). This appointment is from the award date through the life of the Contract, to include close out, unless rescinded or transferred. As the COR, your primary duty is to monitor the Contractor's performance to ensure that all of the technical requirements under the contract are met by the delivery date or within the period of performance, and at the price or within the ceiling stipulated in the contract.

In the performance of the duties delegated to you in this letter, you are cautioned that you could be held personally liable for actions taken or directions given by you to the Contractor that are beyond the authorities given to you in this letter. The duties or authorities in this letter are not re-delegable; therefore, you must advise the Contracting Officer or the Contract Specialist immediately when you are unable to perform these duties.

Your duties and limitations, as applicable to the contract you will be monitoring, are as follows:

MONITORING AND EVALUATING PERFORMANCE

Ensure that the Contractor complies with all of the requirements of the statement of work, specifications, or performance work statement. When requested by the Contractor, provide technical assistance within the scope of the contract (e.g., interpreting specifications, statement of work, performance work statement, etc.). When a difference of opinion between you and the Contractor occurs, notify the Contracting Officer and/or the Contract Specialist immediately for resolution.

If the contract requires Key Personnel, the COR shall ensure that the personnel being used by the Contractor meet the requirements of the position. Review and approve travel and other direct cost (ODC) prior to the Contractor incurring those expenses. Any decrease in or lack of performance shall be brought to the attention of the Contracting Officer and/or Contract Specialist.

If applicable and in accordance with FAR 42.302, the COR shall monitor contractor compliance with specifications or other contractual requirements requiring the delivery or use of environmentally preferable products, energy-efficient products, products containing recovered materials, and bio-based products.

In accordance in Federal Acquisition Circular (FAC) 2005-34 and OMB Memorandum "Improving the Use of Contractor Performance Information" on July 29, 2009, CORs are responsible for entering past performance into the Past Performance Information Retrieval System (PPIRS) annually.

MONITORING COSTS

Review and evaluate the Contractor's progress in relation to the expenditures. When the costs expended by the Contractor are not commensurate with the Contractor's progress, request a meeting with the Contractor and client in an attempt to resolve. If a resolution cannot be found, bring this to the attention of the Contracting Officer and/or Contract Specialist for immediate action.

Review and approve invoices using the rates and other fees established in the contract. Review the Contractor's invoices/vouchers for reasonableness and applicability to the contract and recommend approval or rejection for payment.

CHANGES TO THE CONTRACT

You cannot authorize the Contractor to stop work, and you are not authorized to delete, change, waive, or negotiate any of the technical requirements or other terms and conditions of the contract. Should a change (monetary or otherwise) to the contract become necessary, it must be made by a contract modification issued by the Contracting Officer. When in doubt, contact the Contracting Officer and/or Contract Specialist.

Any contract change requested by the Contractor must be put in writing by the Contractor to the Contracting Officer for action. If, however, you become aware of an impending change, you should immediately advise the Contracting Officer or Contract Specialist. When the proposed change is received by the Contracting Officer, you will be required to provide the Contracting Officer with a written analysis and rationale for the change and to evaluate any costs associated with the change.

You must also recognize and report to the Contracting Officer any Government-required changes to the contract (e.g., items or work no longer required, changes in the specifications, etc.).

INSPECTION OF CONTRACT ITEMS

Perform, in accordance with the terms of the contract, inspection, acceptance, or rejection of the services or deliverables under the contract. The COR must prepare, in writing, a written acceptance or rejection, provide it to the Contractor, and store a copy on the FEDSIM common drive. Immediately notify the Contracting Officer of all rejections and the reason for the action.

Review progress reports from the Contractor and advise the Contracting Officer of any Contractor problems or action required to be taken by the Government.

STANDARDS OF CONDUCT AND CONFLICT OF INTEREST

To avoid improper business practices and personal conflicts of interest and to deal with their apparent or actual occurrences, the COR shall sign any applicable non-disclosure forms. The COR shall also immediately report any potential conflict of interest to their supervisor.

CONTRACT FILE CONTENT AND MAINTENANCE

Establish and maintain an organized contract administration file to record all Contractor and Government actions pertaining to the contract. The file must also include a copy of the COR Letter of Appointment and other documents describing the COR duties; a copy of the contract administration functions delegated to the contract administration office, which may not be delegated to the COR; and documentation of COR actions taken in accordance with the delegation of authority. The files should be organized and saved on the FEDSIM common drive.

CONTRACT CLOSEOUT

Within 30 days after the Contractor has met all terms and conditions of the contract, you must evaluate the Contractor's performance using the information contained in General Services Administration Regulation (GSAR) 542.1503-71 (sample format attached).

Please acknowledge receipt and acceptance of this appointment by signing below. Please direct any questions you may have on this delegation to the Contracting Officer or Contract Specialist.

I understand and accept my assignment as the Contracting Officer's Representative (COR)

X

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Note: This checklist follows the standard format of GSAM 542.1542.15 and content requirements of GSAM 542.15. The checklist may be tailored for the specific contract type. Any “NO” responses noted below shall be accompanied with a statement explaining the observation(s). For each observation(s) provide a recommendation to correct the non-compliance. Observations identify areas of non-compliance and do require response (and action plans, if applicable). Positive observations may be general or specific and may be suitable for replication across the agency as good practices.

Contractor Performance Information

Timeliness of delivery or performance	Yes	No	NA
(1) Adherence to contract delivery schedules.			
(2) Resolution of delays.			
(3) Number of “show cause” letters and “cure notices” issued.			
(4) Number of delinquent deliveries.			
(5) Number of contract extensions resulting from contractor-caused delays.			
(6) Timely submission or performance or required tests.			
(7) Other.			
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Conformance of product or service to contract requirements	Yes	No	NA
(1) Quality of workmanship.			
(2) Reliability.			
(3) Adequacy of correction of defects.			
(4) Number of safety defects.			
(5) Number of product rejections.			
(6) Results of laboratory tests.			
(7) Number and extent of warranty problems.			
(8) Other.			
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Customer comments	Num	Qty	NA
(1) Number and quality of positive comments.			
(2) Number and nature of complaints.			
(3) Adequacy of resolving customer complaints.			
(4) Other.			
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Terminations for default	Yes	No	NA
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

On-the-job safety performance record, including the number of lost or restricted workdays due to occupational injuries in comparison to the national average	Yes	No	NA
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Adequacy of contractor's quality assurance system	Yes	No	NA
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Compliance with other key contract provisions	Yes	No	NA
(1) Subcontracting program			
(2) Labor standards			
(3) Safety standards.			
(4) Reporting requirements			
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Exhibiting customer-oriented behavior	Yes	No	NA
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Other performance elements identified	Yes	No	NA
<u>Observations (specify item #):</u>			
<u>Recommendations:</u>			

Indefinite Delivery, Indefinite Quantity (IDIQ)

United States Cyber Command (USCYBERCOM)

Labor Category (LCAT) Descriptions

September 2015

Table of Contents

Overview	9
1. Administrative Specialist Level I, II, and III	10
The Level I Administrative Specialist	10
The Level II Administrative Specialist	11
The Level III Administrative Specialist.....	11
2. Business Process Engineer Level I, II, and III.....	13
The Level I Business Process Engineer	13
The Level II Business Process Engineer.....	14
The Level III Business Process Engineer	14
3. Collection Manager Level I, II, and III	16
The Level I Collection Manager	16
The Level II Collection Manager.....	17
The Level III Collection Manager	17
4. Configuration Manager Level I, II, and III	18
The Level I Configuration Manager	18
The Level II Configuration Manager	19
The Level III Configuration Manager.....	19
5. Cybersecurity Developer Level I, II, and III	21
The Level I Cybersecurity Developer.....	22
The Level II Cybersecurity Developer.....	22
The Level III Cybersecurity Developer	23
6. Cybersecurity Engineer Level I, II, and III	24
The Level I Cybersecurity Engineer	24
The Level II Cybersecurity Engineer.....	25
The Level III Cybersecurity Engineer	26
7. Cybersecurity Network Architect Level I, II, and III.....	28
The Level I Cybersecurity Network Architect.....	28

The Level II Cybersecurity Network Architect	29
The Level III Cybersecurity Network Architect	29
8. Cyberspace Analyst Level I, II, and III.....	31
The Level I Cyberspace Analyst.....	31
The Level II Cyberspace Analyst.....	32
The Level III Cyberspace Analyst	33
9. Cyberspace Fires (Targets) Analyst Level I, II, and III	34
The Level I Cyberspace Fires (Targets) Analyst	34
The Level II Cyberspace Fires (Targets) Analyst.....	35
The Level III Cyberspace Fires (Targets) Analyst.....	36
10. Cyberspace Intelligence Analyst Level I, II, and III	37
The Level I Cyberspace Intelligence Analyst	37
The Level II Cyberspace Intelligence Analyst.....	38
The Level III Cyberspace Intelligence Analyst	38
11. Cyberspace Joint Operation Planner Level I, II, and III	39
The Level I Cyberspace Joint Operation Planner	39
The Level II Cyberspace Joint Operation Planner	40
The Level III Cyberspace Joint Operation Planner.....	41
12. Cyberspace Operations Engineer Level I, II, and III	43
The Level I Cyberspace Operations Engineer	43
The Level II Cyberspace Operations Engineer	44
The Level III Cyberspace Operations Engineer.....	44
13. Cyberspace Policy Analyst Level I, II, and III	46
The Level I Cyberspace Policy Analyst.....	46
The Level II Cyberspace Policy Analyst	47
The Level III Cyberspace Policy Analyst.....	47
14. Cyberspace Scientist Level I, II, and III.....	49
The Level I Cyberspace Scientist.....	49

The Level II Cyberspace Scientist	50
The Level III Cyberspace Scientist.....	50
15. Cyberspace Training Facilitator Level I, II, and III.....	52
The Level I Cyberspace Training Facilitator	52
The Level II Cyberspace Training Facilitator	53
The Level III Cyberspace Training Facilitator.....	53
16. Cyberspace Training Specialist Level I, II, and III.....	54
The Level I Cyberspace Training Specialist	54
The Level II Cyberspace Training Specialist.....	55
The Level III Cyberspace Training Specialist	55
17. Graphic Artist Level I, II, and III.....	56
The Level I Graphic Artist.....	56
The Level II Graphic Artist.....	57
The Level III Graphic Artist	57
18. Graphic Designer Level I, II, and III.....	58
The Level I Graphic Designer.....	58
The Level II Graphic Designer	58
The Level III Graphic Designer	59
19. Information Technology Specialist Level I, II, and III.....	60
The Level I Information Technology Specialist	61
The Level II Information Technology Specialist.....	62
The Level III Information Technology Specialist.....	63
20. Inspector General Specialist Level I, II, and III.....	64
The Level I Inspector General Specialist.....	64
The Level II Inspector General Specialist.....	64
The Level III Inspector General Specialist	65
21. Intelligence Planner Level I, II, and III.....	66
The Level I Intelligence Planner.....	66

The Level II Intelligence Planner.....	67
The Level III Intelligence Planner s.....	67
22. Knowledge Management Specialist Level I, II, and III	68
The Level I Knowledge Management Specialist	68
The Level II Knowledge Management Specialist.....	68
The Level III Knowledge Management Specialist.....	69
23. Legislative Affairs Specialist Level I, II, and III	71
The Level I Legislative Affairs Specialist	71
The Level II Legislative Affairs Specialist	72
The Level III Legislative Affairs Specialist.....	72
24. Malware Analyst Level I, II, and III.....	73
The Level I Malware Analyst	73
The Level II Malware Analyst	74
The Level III Malware Analyst.....	74
25. Modeling & Simulation Engineer Level I, II, and III	76
The Level I Modeling & Simulation Engineer	76
The Level II Modeling & Simulation Engineer	76
The Level III Modeling & Simulation Engineer.....	77
26. Network Engineer Level I, II, and III.....	78
The Level I Network Engineer.....	78
The Level II Network Engineer	79
The Level III Network Engineer.....	79
27. Open Source Analyst Level I, II, and III.....	81
The Level I Open Source Analyst.....	81
The Level II Open Source Analyst	81
The Level III Open Source Analyst.....	82
28. Operational Design Cognitive Operator Level I, II, and III	83
The Level I Operational Design Cognitive Operator.....	83

The Level II Operational Design Cognitive Operator.....	83
The Level III Operational Design Cognitive Operator	84
29. Operations Research Analyst Level I, II, and III.....	85
The Level I Operations Research Analyst	85
The Level II Operations Research Analyst.....	86
The Level III Operations Research Analyst.....	87
30. Project Analyst Level I, II, and III.....	88
The Level I Project Analyst	88
The Level II Project Analyst.....	89
The Level III Project Analyst.....	89
31. Program Manager Level I, II, and III	91
The Level I Program Manager	91
The Level II Program Manager.....	92
The Level III Program Manager	92
32. Project Manager Level I, II, and III	94
The Level I Project Manager	94
The Level II Project Manager	95
The Level III Project Manager.....	95
33. Public Affairs Specialist Level I, II, and III.....	97
The Level I Public Affairs Specialist.....	97
The Level II Public Affairs Specialist.....	98
The Level III Public Affairs Specialist	98
34. Records Management Specialist Level I, II, and III	99
The Level I Records Management Specialist	99
The Level II Records Management Specialist	100
The Level III Records Management Specialist.....	100
35. SharePoint Developer Level I, II, and III.....	101
The Level I SharePoint Developer.....	101

The Level II SharePoint Developer	101
The Level III SharePoint Developer	102
36. SIGINT Policy Analyst Level I, II, and III	103
The Level I SIGINT Policy Analyst	103
The Level II SIGINT Policy Analyst	103
The Level III SIGINT Policy Analyst	104
37. Software Developer Level I, II, and III	105
The Level I Software Developer	106
The Level II Software Developer	107
The Level III Software Developer	108
38. Special Security Officer Specialist Level I, II, and III	109
The Level I Special Security Officer Specialist	109
The Level II Special Security Officer Specialist	110
The Level III Special Security Officer Specialist	110
39. Subject Matter Expert Level I, II, and III	111
The Level I Subject Matter Expert	111
The Level II Subject Matter Expert	112
The Level III Subject Matter Expert	113
40. Systems Administrator Level I, II, and III	114
The Level I Systems Administrator	114
The Level II Systems Administrator	114
The Level III Systems Administrator	115
41. Systems Engineer Level I, II, and III	116
The Level I System Engineer	116
The Level II System Engineer	117
The Level III System Engineer	117
42. Systems Integrator Level I, II, and III	119
The Level I Systems Integrator	119

The Level II Systems Integrator.....	119
The Level III Systems Integrator	120
43. Technical Writer Level I, II, and III.....	121
The Level I Technical Writer.....	121
The Level II Technical Writer	121
The Level III Technical Writer	122
44. Test Engineer Level I, II, and III	123
The Level I Test Engineer.....	124
The Level II Test Engineer	124
The Level III Test Engineer	125
45. Web Developer Level I, II, and III.....	126
The Level I Web Developer.....	126
The Level II Web Developer	126
The Level III Web Developer	127
ACRONYM LIST	128

USCYBERCOM

Indefinite Delivery/Indefinite Quantity (IDIQ)

LABOR CATEGORY DESCRIPTIONS

Overview

The United States Cyber Command (USCYBERCOM) Indefinite Delivery Indefinite Quantity (IDIQ) Contract Task Orders (TO) must be staffed by personnel who meet the requirements defined in the labor categories described below. Personnel filling Level II positions must meet all Level I and Level II position requirements. Personnel filling Level III positions must meet all Level I, Level II, and Level III position requirements. The Contracting Officer (CO) may waive position requirements on a case-by-case basis if the candidate has similar requisite experience and/or other qualifications. The maximum labor rate associated with each position will be fixed for the term of the contract. Under no circumstance shall a labor rate exceed the maximum rate defined in this IDIQ contract. Labor category descriptions are provided below.

For all labor categories, unless otherwise specified, the following education degrees may be substituted for years of experience:

Bachelor's Degree = One year of experience

Master's Degree = Two years of experience

Ph.D. = Three years of experience

If a minimum education requirement is cited, the minimum degree may not be substituted for experience. For example, if the minimum requirement is a Bachelor's Degree, then a one year substitution for experience does not meet the requirement.

For all labor categories, unless otherwise specified, five years of additional experience may be substituted for a Bachelor's Degree. For example, if the minimum requirement is a Bachelor's Degree and five years of experience, then a high school diploma and 10 years of experience meets the requirement.

1. Administrative Specialist Level I, II, and III

Labor Category	Description
Administrative Specialist	<ul style="list-style-type: none">• Performs all aspects of administrative and office support activities for the directorates, divisions, and/or branches within USCYBERCOM• Coordinates among organizations for day-to-day operations• Assists with planning and coordinating activities for office relocations and prepares front office materials for relocations• Maintains organization documentation, records, and files in accordance with knowledge management and records management policies and procedures

The Level I Administrative Specialist

- Provides end-user support and performs general administrative duties with minimal guidance
- Utilizes Command internal systems to collect, analyze, and compile metrics for division and or branch reports
- Assists with the preparation of management plans and reports
- Assists with maintaining knowledge management files and websites for the organization
- Interfaces with personnel to maintain logs, records, and files
- Develops and maintains calendars and schedules
- Assists with coordinating, planning, and organizing meeting events, and supports planning and execution of technical exchanges, conferences, and synchronization sessions, obtaining space and necessary materials and equipment
- Contributes to the review, development, and management of office administrative operating procedures
- Assists with the preparation and/or distribution of read-ahead materials and briefings for a wide-range of audiences at various military ranks and civilian levels
- Records and distributes meeting minutes
- Prepares, submits, and tracks expense reports
- Submits visit requests
- Tracks formal USCYBERCOM task items and reports status

- Assists in budgetary, billing, and financial management of front office expenses incurred to support the organization (e.g., office supplies)

Qualifications:

- Minimum three years of experience in office administration
- Minimum of High School Diploma
- Proficient in Microsoft Office and Outlook
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Administrative Specialist

- Provides end-user support and performs administrative duties with no guidance
- Assists with coordinating, planning, and organizing events to include technical exchanges, conferences, and synchronization sessions, obtaining space and necessary materials and equipment
- Works independently and communicates orally and in writing with all levels of an organization
- Coordinates the arrival of visitors to include senior level military and civilian personnel and foreign visitors
- Performs analysis, development, and update of command or office administrative operating procedures

Qualifications:

- Minimum six years of experience in office administration
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Administrative Specialist

- Initiates action to provide end-user support and performs complex administrative duties
- Contributes to and conducts technical editing of reports and briefs
- Coordinates, plans, and organizes significant and large events, to include obtaining space and necessary materials and equipment
- Coordinates the administrative specialist team

Qualifications:

- Minimum 10 years of experience in office administration
- Minimum of High School Diploma
- Proficient in Microsoft Office and Outlook
- Strong attention to detail and organizational skills. Excellent communications skills.

2. Business Process Engineer Level I, II, and III

Labor Category	Description
Business Process Engineer	<ul style="list-style-type: none"> • Provide analysis and recommendations in support of mission-oriented business functions and related applications and systems • Aligns processes, systems, policies, and organizational structures with mission and strategy of the organization and Command • Analyzes workflows and processes to identify process inefficiencies and areas for improvement • Creates process change by integrating new processes to improve existing ones and communicating these changes to impacted stakeholders • Develops innovative solutions • Recommends and facilitates quality improvement efforts • Plans and implements approved business solutions and develops metrics, and methods to collect those metrics, to measure operational efficiency

The Level I Business Process Engineer

- Provides technical assistance throughout business process improvement and modernization efforts to reengineer methodologies and principles, including associated processes, technology, organization structure(s), skills, and organizational culture
- Conducts research, evaluations, studies, and analysis with minimal guidance
- Provides technical assistance to develop change management plans, reports, processes, business policy, regulations, and standard operating procedures (SOPs) with minimal guidance
- Has a general understanding of activity data modeling, transaction flow analysis, internal control and risk analysis, modern business methods, and performance measure techniques
- Has a general understanding of Lean Six Sigma and Process Change Management principles to reengineer processes, reduce redundancy, and increase efficiency
- Provides technical assistance with establishing requirements for information systems required to facilitate and support business process improvements, procedures, and with the development and application of organizational-wide information models

Qualifications:

- Minimum two years of experience participating in Business Process Reengineering (BPR)

activities with one of the two years of experience using process improvement methodologies, e.g., Lean Six Sigma

- Minimum of Bachelor's Degree from an accredited college or university in a business discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Business Process Engineer

- Contributes substantive content throughout business process improvement and modernization efforts to reengineer methodologies and principles, including associated processes, technology, organization structure(s), skills, and organizational culture
- Conducts research, evaluations, studies, and analysis with no guidance
- Contributes substantive content to change management plans, reports, processes, business policy, regulations, and SOPs with minimal guidance
- Has an in-depth understanding of activity data modeling, transaction flow analysis, internal control and risk analysis, modern business methods, and performance measure techniques
- Has an in-depth understanding of Lean Six Sigma and Process Change Management principles to reengineer processes, reduce redundancy, and increase efficiency
- Contributes substantive content to define requirements for information systems required to facilitate and support business process improvements, procedures, and with the development and application of organizational-wide information models
- Develops budget estimates and resource estimates in support of business process reengineering efforts
- Processes large volumes of complex data rapidly and accurately and translates highly technical and programmatic data into actionable reports
- Leverages industry best practices to plan, organize, and guide complex requirements using Commercial Off-The-Shelf (COTS) tools

Qualifications:

- Minimum five years of experience participating in BPR activities with two of the five years of experience using process improvement methodologies, e.g., Lean Six Sigma
- Minimum of Bachelor's Degree from an accredited college or university in a business discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Business Process Engineer

- Coordinates business process improvement and modernization efforts to methodologies and principles, including associated processes, technology, organization structure(s), skills, and

organizational culture

- Initiates action to conduct research, evaluations, studies, and analysis
- Coordinates efforts to develop change management plans, reports, processes, business policy, regulations, and SOP with minimal guidance
- Has a thorough understanding of activity data modeling, transaction flow analysis, internal control and risk analysis, modern business methods and performance measure techniques
- Has a thorough understanding of Lean Six Sigma and Process Change Management principles to reengineer processes, reduce redundancy and increase efficiency
- Coordinates efforts to define requirements for information systems required to facilitate and support business process improvements, procedures, and with the development and application of organization-wide information models
- Coordinates efforts to integrate new processes with existing ones and communicate changes to all stakeholders. Key coordinator between project teams to ensure enterprise-wide integration of reengineering efforts.

Qualifications:

- Minimum 10 years of experience participating in BPR activities with five of the 10 years of experience using process improvement methodologies, e.g., Lean Six Sigma
- Minimum of Bachelor's Degree from an accredited college or university in a business discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

3. Collection Manager Level I, II, and III

Labor Category	Description
Collection Manager	<ul style="list-style-type: none">• Collects, documents, and recommends prioritization of Command intelligence requirements• Tracks sources to ensure relevancy, eliminating duplication of effort, and feeding data into various organizations based on the need• Conducts gap analysis and reports on collected data to aid in the decision making process for leadership and other stakeholders• Supports the development and implementation of collection strategies for stakeholders and recommends innovative solutions to enhance collection activities to meet priorities and close gaps• Supports the preparation, production, and coordination of written products and briefings for stakeholders• Maintains updated documentation depicting sources of data from internal, open source, and third-party sources• Researches intelligence collection issues that cross disciplines, organizational boundaries, or functional topic areas

The Level I Collection Manager

- Provides stakeholder support and performs general collection manager duties with minimal guidance
- Possesses a general understanding of Collection Management basic concepts
- Utilizes Command internal systems to collect, analyze, and compile data and metrics
- Assists with the preparation of reports and briefings
- With minimal guidance, interfaces with stakeholders and coordinates actions
- Contributes to the review, development, implementation, and management of collection strategies

Qualifications:

- Minimum three years of experience in collection management
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Collection Manager

- Provides stakeholder support and performs a vast array of collection manager duties with no guidance
- Possesses an in-depth understanding of Collection Management concepts
- Contributes substantive content for reports and briefings
- With no guidance, interfaces with stakeholders and coordinates actions
- Contributes substantive content to the review, development, implementation, and management of collection strategies

Qualifications:

- Minimum six years of experience in collection management
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Collection Manager

- Initiates stakeholder support and performs expansive collection manager duties
- Possesses a thorough understanding of Collection Management concepts
- Develops reports and briefings
- Enhances stakeholder relationships and initiates the coordination of actions
- Reviews, develops, implements, and manages collection strategies

Qualifications:

- Minimum 10 years of experience in collection management
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

4. Configuration Manager Level I, II, and III

Labor Category	Description
Configuration Manager	<ul style="list-style-type: none">• Conducts configuration management (CM) planning and describes provisions for configuration identification, change control, configuration status accounting, and configuration audits• Develops documentation for CM planning and activities• Identifies and maintains the original and subsequent configuration versions of requirements documentation, design documentation, and network/software/other related documentation• Manages configuration change control and regulates the change process so that only approved and validated changes are incorporated into product documents and related hardware and software

The Level I Configuration Manager

- Provides technical assistance for maintaining and developing the CM environment for hardware and software product build, staging, testing, and integration
- Has a general understanding of the basic concepts of defining hardware and software configuration processes and procedures
- Conducts configuration status accounting, and tracks and reports all CM problems and changes in product documents/software
- Conducts configuration audits and supports audits to verify that requirements of all baselines have been met by the as-built software
- Provides technical assistance for software quality assurance process audits
- With minimal guidance, defines, documents and maintains the Configuration Control Board (CCB), including roles and responsibilities of CCB members
- With minimal guidance, defines hardware and software configuration processes and procedures, version control processes, and policies and procedures to ensure they are followed on hardware and software development projects
- Assists with the use of CM tools to store, track, and manage configuration items

Qualifications:

- Minimum two years of experience in CM
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university
- Minimum Department of Defense (DOD) 8140/DOD 8570 Information Assurance Technical (IAT) Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Configuration Manager

- Contributes substantive content for maintaining and developing the CM environment for hardware and software product build, staging, testing, and integration
- Has an in-depth understanding of the concepts of defining hardware and software configuration processes and procedures
- Contributes substantive content for software quality assurance process audits
- With no guidance, define, document, and maintain the CCB, including roles and responsibilities of CCB members
- With no guidance, defines hardware and software configuration processes and procedures, version control processes, policies, and procedures to ensure they are followed on hardware and software development projects
- Utilizes CM tools to store, track, and manage configuration items

Qualifications:

- Minimum five years of experience in CM
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Configuration Manager

- Coordinates software quality assurance process audit definition and activities
- Initiates actions to define, document, and maintain the CCB, including roles and responsibilities of CCB members
- Initiates actions to define hardware and software configuration processes and procedures, version control processes, policies, and procedures to ensure they are followed on hardware and software development projects

Qualifications:

- Minimum 10 years of experience in configuration management
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

5. Cybersecurity Developer Level I, II, and III

Labor Category	Description
Cybersecurity Developer	<ul style="list-style-type: none"> • Develops security software and ensures security is implemented during software development • Conceives, proposes, and designs software security to mitigate weaknesses and vulnerabilities • Researches and tests new security technologies and processes to enhance security capabilities • Analyzes and assesses infrastructures for potential vulnerabilities that may result from improper configurations, hardware or software flaws, or operational weaknesses • Performs security monitoring, log analysis, and forensic analysis to detect security incidents and mount incident response • Assesses and reports on the impact of security issues that are discovered; recommends and develops mitigation strategies or technical solutions • Assesses system information security policies against client policies • Ensures policies are comprehensive to the system • Evaluates security components against their ability to resist threats in the deployed environment, evaluates configurations and implementation of firewalls, proxy servers, routers, Virtual Private Networks (VPNs), Intrusion Detection Systems (IDS), wireless networks, etc., against policy requirements, industry best practices, and vendor recommendations • Plans and integrates the installation of new or modified security hardware, operating systems, and software applications • Conducts vulnerability assessments and penetration testing customized to system functionality and technical requirements, and based on status within security assessment and authorization cycle and authority to operate status • Perform computer network exploitation development: embedded reverse engineering, vulnerability research, and application development for software and embedded systems with a focus on Offensive Cyber Operations (OCO) and Defensive Cyber Operations (DCO) activities

- Develops test plans and tests software security mechanisms for operational effectiveness and deployment readiness; develops test and evaluation reports

The Level I Cybersecurity Developer

- Develops security software with minimal guidance
- Identifies and develops improvements to security controls currently in place with minimal guidance
- Possesses a general understanding of software security and security technologies and concepts
- Contributes to the development of tests plans and evaluation reports, and assists during activities for testing software security mechanisms for operation effectiveness and deployment readiness
- Assists in the conduct of vulnerability assessments and penetration test activities
- Evaluates processes and procedures to integrate and enhance security capabilities in test and operational environments

Qualifications:

- Minimum five years of experience as a Cybersecurity Developer or related functional area
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Cybersecurity Developer

- Develops security software with no guidance
- Identifies and develops improvements to security controls currently in place with no guidance
- Possesses an in-depth understanding of software security and security technologies and concepts
- Contributes substantive content to the development of test plans and evaluation reports, and conducts activities for testing software security mechanisms for operation effectiveness and deployment readiness
- Conducts vulnerability assessments and penetration test activities with no guidance

Qualifications:

- Minimum 10 years of experience as a Cybersecurity Developer or related functional area
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Cybersecurity Developer

- Provides direction and/or recommendations, and develops security software and improvements of security controls currently in place
- Possesses a thorough understanding of software security and security technologies and concepts
- Develops test plans and evaluation reports, and conducts activities for testing software security mechanisms for operation effectiveness and deployment readiness
- Prepares the environment and conducts vulnerability assessments and penetration test activities

Qualifications:

- Minimum 15 years of experience as a Cybersecurity Developer or related functional area
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

6. Cybersecurity Engineer Level I, II, and III

Labor Category	Description
Cybersecurity Engineer	<ul style="list-style-type: none">• Ensures the rigorous application of cybersecurity policies, principles, and practices in the delivery of all Information Technology (IT) and cybersecurity services• Develops and designs security solutions to maintain confidentiality, integrity, and availability of information throughout the enterprise• Identifies, plans, and documents improvements to security controls currently in place• Develops and documents recommendations and courses of action (COAs) to solve complex cybersecurity problems• Develops and interprets cybersecurity requirements as part of the IT acquisition development process and assists in the formulation of cybersecurity/IT budgets• Plans and schedules the installation of new or modified security hardware, operating systems, and software applications• Ensures the assessment and implementation of identified computer and network environment fixes such as system patches and fixes associated with specific technical vulnerabilities as part of the Cybersecurity Vulnerability Management program• Guides the implementation of appropriate operational structures and processes to ensure an effective cybersecurity program, including boundary defense, incident detection, and response

The Level I Cybersecurity Engineer

- Possesses a general understanding of the basic concepts of cyber engineering and cybersecurity
- Maintains general working knowledge and understanding of the DOD cybersecurity policies and the Risk Management Framework
- With minimal guidance, conducts cybersecurity engineering research and analysis and provides recommendations for the implementation of security mechanisms
- Provides technical assistance to the development of cybersecurity documentation, concept papers, and test plans required by Command policies, and the Risk Management Framework
- Establishes and maintains effective working relationships with other Government agencies

and mission partners

- Develops and delivers articulate and effective briefings/presentations on general and comprehensive cybersecurity engineering topics as applicable to assigned projects
- With minimal guidance, evaluates functional operation and performance in light of test results and makes recommendations regarding Certification and Accreditation (C&A)

Qualifications:

- Minimum five years of experience with cybersecurity or information assurance
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 Information Assurance Management (IAM) Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Cybersecurity Engineer

- Possesses an in-depth understanding and the ability to apply intermediate concepts of cyber engineering and cybersecurity
- Maintains in-depth knowledge and understanding of the DOD cybersecurity policies and the Risk Management Framework
- With no guidance, conducts cybersecurity engineering research and analysis, provides recommendations for the implementation of security mechanisms, and provides educational briefings on the recommended cybersecurity mechanism
- Contributes substantive content to the development of cybersecurity documentation, concept papers, and test plans required by Command policies and the Risk Management Framework
- Maintains comprehensive knowledge and understanding of DOD and/or Intelligence Community (IC) engineering efforts, across multiple engineering disciplines
- With no guidance, evaluates functional operation and performance in light of test results and makes recommendations regarding C&A

Qualifications:

- Minimum 10 years of experience with cybersecurity or information assurance
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline

- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Cybersecurity Engineer

- Possesses a thorough understanding and ability to apply intermediate concepts of cyber engineering and cybersecurity
- Maintains thorough knowledge and understanding of the DOD cybersecurity policies and the Risk Management Framework
- Initiates actions to conduct cybersecurity engineering research and analysis and provides recommendations for the implementation of security mechanisms
- Initiates actions to apply advanced concepts of cyber engineering and cybersecurity to development and architecture projects
- Coordinates effort to develop cybersecurity documentation, concept papers, and test plans required by Command policies and the Risk Management Framework
- Analyzes complex information independently and takes appropriate actions, and reviews and implements recommendations from others
- Maintains extensive knowledge and understanding of DOD and/or IC engineering efforts, across multiple engineering disciplines
- Develops and delivers articulate and effective briefings/presentations on complex cybersecurity engineering topics as applicable to assigned projects to any size audience that may include high-level decision makers
- Prioritizes competing requirements and tasks, and manages long-term and short-term obligations
- Coordinates effort to develop all cybersecurity documentation, concept papers, and test plans required by Command policies and the Risk Management Framework
- Initiates actions to evaluate functional operation and performance in light of test results and makes recommendations regarding C&A
- Effectively provides engineering guidance to cybersecurity engineers Level I and II

Qualifications:

- Minimum 15 years of experience with cybersecurity or information assurance
- Minimum of Bachelor's Degree in a technical or business discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline

- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

7. Cybersecurity Network Architect Level I, II, and III

Labor Category	Description
Cybersecurity Network Architect	<ul style="list-style-type: none">• Assists with the design and implementation of Local Area Networks (LAN), Wide Area Networks (WAN), intranets, extranets, and other data communications networks• Develops enterprise, network, and security architecture designs for all layers of the architecture, including business, data, technology, and services throughout the entire systems engineering and development life cycles• Performs network modeling, analysis, and planning• Researches and recommends network and data communications hardware and software

The Level I Cybersecurity Network Architect

- Possesses general knowledge in the system engineering life cycle and current national cyberspace policy
- Applies a working knowledge of tools, such as System Architect or Sparx, to develop DOD Architecture Framework (DODAF) artifacts (operational views, system views)
- With minimal guidance, develops functional requirements and specification documents
- Provides enterprise and system security engineering and assessment of system security engineering products and solutions and C&A activities
- Analyzes system and network security designs and conducts risk assessments
- Translates business and security objectives into technology designs
- Conducts data gathering and research, extracts network architecture requirements from stakeholders, and documents and incorporates the requirements into network design documents
- Works collaboratively with engineering partners and team members
- Possesses general knowledge and understanding of virtualization and cloud computing

Qualifications:

- Minimum five years of experience as a Cybersecurity Network Architect or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in IT, Computer Science, Cybersecurity, Computer Engineering, or related discipline

- Minimum DOD 8140/DOD 8570 Information Assurance System Architect and Engineer (IASAE) Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Cybersecurity Network Architect

- Possesses in-depth knowledge in the system engineering life cycle and current national cyberspace policy
- With no guidance, develops functional requirements and specification documents
- Develops and designs infrastructures necessary to support system development strategies and technology roadmaps
- Advises on the feasibility of potential future projects to the Government Program Manager
- Advises on the purchase of technology products
- Develops network and security architectures and methodologies and conducts emerging cybersecurity, information security, and technology analyses

Qualifications:

- Minimum 10 years of experience as a Cybersecurity Network Architect or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in IT, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IASAE Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Cybersecurity Network Architect

- Possesses thorough knowledge in the system engineering life cycle and current national cyberspace policy
- Initiates activities to develop functional requirements and specification documents
- Develops and presents technology roadmaps
- Develops implementation plans and project timelines
- Conducts cost/benefit analysis of architecture designs
- Develops cost estimates and network designs specifications
- Develops 'as-is' and 'to-be' architecture designs and transition plans between the current state

and target architecture

- Serves as Subject Matter Expert (SME) in architecture working groups, presents architecture solutions, methodologies, and frameworks, and coordinates/negotiates toward a solution

Qualifications:

- Minimum 15 years of experience as a Cybersecurity Network Architect or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in IT, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

8. Cyberspace Analyst Level I, II, and III

Labor Category	Description
Cyberspace Analyst	<ul style="list-style-type: none"> • Provides technical expertise for the identification, development and prioritization of cyberspace operations requirements, processes, procedures, and governing directives • Assists in conducting cyberspace operations and defense of the DOD Information Network (DODIN) • Provides situational awareness (SA) of cyber incidents, health, performance, availability, and reliability of the DODIN • Identifies issues and priorities affecting operations • Supports the creation, dissemination, and compliance of applicable orders and directives to the DOD community • Addresses areas of concern for the development of cyberspace capabilities for cyberspace operations • Prepares and modifies requirements to develop cyberspace capabilities based on the changing cyberspace environment for appropriate Government review, validation, and prioritization • Analyzes capability development requirements, concept of operation documents, and system architectures

The Level I Cyberspace Analyst

- Creates, disseminates, and tracks status of USCYBERCOM Orders and Directives
- Prepares SA and operational update briefs
- Reviews open source reporting for new vulnerabilities, malware, or other threat that have the potential to impact the DODIN
- Participates and provides input for Command exercises
- Utilizes USCYBERCOM capabilities in order to monitor, track, detect, and analyze cyber threat activities

Qualifications:

- Minimum three years of experience as a Cyberspace Analyst or a related functional area
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level I Certification

- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Analyst

- Utilizes automated capabilities to assess risk to DODIN assets
- Assists in identifying and prioritizing requirements for capability development efforts
- Analyzes proposed capabilities, recommends COAs, and develops solutions to address areas of concern for shortfalls
- Develops, maintains, and automates metrics to assess USCYBERCOM operational Measure of Effective and Performance (MOE/MOP)
- Develops concept papers, technical white papers, and related documentation detailing cyber security practices for implementation throughout DOD
- Analyzes vulnerabilities with known exploits that do not have vendor-provided mitigation or remediation action
- Conducts research that focuses on rapidly emerging cyber threats and cyber adversary Tactics, Techniques, and Procedures (TTPs)
- Collaborates with internal and external partners to facilitate cyber SA and information sharing
- Assesses the development of cyberspace capabilities to validate USCYBERCOM requirements

Qualifications:

- Minimum six years of experience as a Cyberspace Analyst or a related functional area
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Analyst

- Plans, organizes, determines, and recommends necessary policies, regulations, directives, programs, doctrine, and procedures for the establishment and maintenance of assigned and anticipated changes to the DODIN
- Tests and documents results for newly developed capabilities based on USCYBERCOM requirements
- Develops, integrates, and maintains operational TTPs, SOPs, and Concept of Operations (CONOPs)
- Identifies, analyzes, and develops mitigation or remediation actions for system and network vulnerabilities
- Develops and assesses current DODIN plans and policies to include emerging technologies
- Synchronizes and prioritizes capability requirements and new tactical uses of existing capabilities
- Identifies shortfall and capability gaps on DOD policy and guidance

Qualifications:

- Minimum 10 years of experience as a Cyberspace Analyst or a related functional area
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level III Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

9. Cyberspace Fires (Targets) Analyst Level I, II, and III

Labor Category	Description
Cyberspace Fires (Targets) Analyst	<ul style="list-style-type: none"> Assists in the coordination of joint strategic and operational planning and execution of joint fires, targeting, capability pairing, and threat mitigation in support of the Cyber Mission Force and other operations Provides advice to leadership on all aspects of joint fires and threat mitigation Provides support to future operations planners to integrate cyber capabilities into plans Plans, organizes, determines, and recommends necessary policies, regulations, directives, programs, doctrine, and procedures for the establishment and maintenance of assigned and anticipated joint fires coordination and execution Supports planning in OCO and DCO throughout the entire Joint Operation Planning Process (JOPP) Synchronizes and deconflicts Special Access Program/Special Technical Operation (SAP/STO) capabilities with operational planning Participates as the Fires SME in exercises Coordinates targeting strategy development and engagement responsibilities with components, subordinates commands, and supporting commands Synchronizes and implements targeting methodologies and prioritization methods Assists with all aspects of cyber advanced targeting, to include interagency planning, joint targeting board support, cyber weapons capability analysis, target systems analysis, target materials production, collateral effects estimate, and joint planning group support

The Level I Cyberspace Fires (Targets) Analyst

- Provides technical assistance and supports the Cyber Tasking Cycle
- Creates, manages, updates, and implements the Master Cyber Operations Plan (MCOP)

- Manages Cyber Tasking Orders (CTOs)
- Attends the Operations Synchronization meetings
- Coordinates with Cyber Mission Forces and other subordinate units in order to facilitate the Cyber Tasking Cycle processes
- Inputs data, including the Joint Tactical Cyber Request (JTCR) updates, into the Command and Control (C2) system, reviews data, and recommends updates to tasking
- Facilitates preparation of the Joint Targeting Working Group (JTWG) and Joint Targeting Coordination Board (JTCB)
- Monitors and facilitates all targeting lists at the intermediate level and above
- Drafts Commander's targeting guidance
- Prepares strike package and Cyber Request and Approval (C-RAP) documents

Qualifications:

- Minimum five years of experience in Fires and/or Targeting
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Fires (Targets) Analyst

- Collaborates with the Defense Information Systems Agency (DISA), National Security Agency (NSA), other interagency organizations and other service providers to ensure that USCYBERCOM and/or Cyber Mission Forces Fires requirements are implemented
- Develops cyber TTPs that advise the future operations planners on achieving Cyberspace Operations effects within the "realm of the possible" in support of operations and exercise objectives
- Acts as technical liaison on behalf of the USCYBERCOM Operations Directorate between capability SMEs and capability developers, capability testers, planning teams, operations support staff, and operating units during planning and operations
- Participates in USCYBERCOM requirements working groups as a capability SME for defined cyber capabilities/tools and/or for targeting
- Acts as a liaison between Fires and Intel regarding the tasking processes and targeting
- Conducts outreach briefs to inform external partners and stakeholders on USCYBERCOM Fires

processes

Qualifications:

- Minimum 10 years of experience in Fires and/or Targeting
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Fires (Targets) Analyst

- Develops documents to include lessons learned, as well as results and conclusions with relevant organizations such as DOD, Federal Agencies, and commercial partners
- Provides scheduled and ad hoc briefings and point papers on Cyberspace Operations
- Develops and conducts briefings to senior personnel on USCYBERCOM Fires processes
- Participates as Senior Fires SME in exercises
- Develops joint targeting policies and procedures
- Advises and recommends supporting processes and procedures for the JTCB

Qualifications:

- Minimum 15 years of experience in Fires and/or Targeting
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

10. Cyberspace Intelligence Analyst Level I, II, and III

Labor Category	Description
Cyberspace Intelligence Analyst	<ul style="list-style-type: none"> • Serves as an Intelligence Specialist with responsibilities for participating in the production of all-source intelligence products pertaining to cyberspace operation and planning activities • Applies a wide range of intelligence analytic skills to monitor, assess, and report on cyberspace operations, capabilities, vulnerabilities, and personalities that could pose a threat to US computers, communications, weapon systems, and operations • Advises stakeholders on key developments in their assigned area, including immediate and long-term responses • Conducts reviews, identifies gaps, recommends solutions, and ensures alignment with strategies • Supports decision making and special projects on the preparation, production, and coordination of written products and briefings for stakeholders and leadership

The Level I Cyberspace Intelligence Analyst

- Contributes to the development of intelligence products and performs cyberspace intelligence analyst duties with minimal guidance
- Possesses a general understanding of intelligence analytic basic concepts to monitor, assess, and report on cyberspace operations, capabilities, and vulnerabilities
- Assists with the preparation of reports and briefings
- With minimal guidance, advises stakeholders and coordinates actions
- Contributes to the development of analytic approaches and recommendations to problems and situations for which data are incomplete, controversial, or which no precedence exists

Qualifications:

- Minimum three years of experience as an Intelligence Analyst, Cyber or Signals Intelligence (SIGINT) focus
- Minimum of High School Diploma

- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Cyberspace Intelligence Analyst

- Contributes to the development of intelligence products and performs a vast array of cyberspace intelligence analyst duties with no guidance
- Possesses an in-depth understanding of intelligence analytic concepts to monitor, assess, and report on cyberspace operations, capabilities, and vulnerabilities
- Contributes substantive content for reports and briefings
- With no guidance, advises stakeholders and coordinates actions
- Contributes substantive content to the development of complex analytic approaches and recommendations to problems and situations for which data are incomplete, controversial, or which no precedence exists

Qualifications:

- Minimum six years of experience as an Intelligence Analyst, Cyber or SIGINT focus
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Cyberspace Intelligence Analyst

- Develops intelligence products and performs expansive cyberspace intelligence analyst duties
- Possesses a thorough understanding of intelligence analytic concepts to monitor, assess, and report on cyberspace operations, capabilities, and vulnerabilities
- Develops reports and briefings
- Enhances stakeholder relationships; advises and coordinates actions
- Develops analytic approaches and recommendations to problems and situations for which data are incomplete, controversial, or which no precedence exists

Qualifications:

- Minimum 10 years of experience as an Intelligence Analyst, Cyber or SIGINT focus
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

11. Cyberspace Joint Operation Planner Level I, II, and III

Labor Category	Description
Cyberspace Joint Operation Planner	<ul style="list-style-type: none"> • Monitors and reviews strategies, doctrine, policies, directives, and instructions from higher echelon headquarters and makes recommendations to ensure compliance and/or consideration in planning efforts • Develops plans and orders through the application of operational art and operational design, and by using the JOPP, within the milestones, deliverables, and interaction points for plans developed using Adaptive Planning and Execution (APEX) activities • Provides input to briefings, transitioning concepts to execution, and assisting in the coordination of joint operational planning in support of training, exercises, combat, and contingency plans and operations • Develops and integrates cyberspace capabilities into deliberate, contingency, operation, and crisis action planning • Provides input for the development of TTPs, CONOPs, COAs, and other related documents related to OCO, DCO, and the securing, operating, and defending of the DODIN • Provides input to address shortfalls, prioritize and validate requirements, and be prepared to modify development planning efforts based on the changing cyberspace environment • Contributes to the development of exercise scenarios, exercise operational plans, and other required documentation to support planning and execution to accomplish USCYBERCOM exercise training priorities • Conducts research of current and emerging threats to U.S. Critical Infrastructure and Key Resources (CIKR) • Participates in Joint Planning Groups (JPGs), and Operational Planning Groups/Teams (OPG/OPTs)

The Level I Cyberspace Joint Operation Planner

- Acts a full participant and provides technical assistance to JPG and, OPG/OPTs developing and integrating cyber capabilities into plans, and in support of Combatant Commander planning efforts
- Knowledgeable of cyberspace operations planning activities coordination through the Integrated

Joint Special Technical Operations (IJSTO), to include Evaluation Request and Response Messages, SAP procedures, and the Review and Approval Process for Cyberspace Operations (RAPCO)

- Exhibits an understanding of operational design, joint operation planning, and APEX
- Possesses a complete understanding of all planning methodologies and applications in all phases of military operations
- Assists with the coordination of joint operation planning in support of combat and contingency operations
- Knowledgeable of and participates in all phases and steps of the JOPP and APEX activities
- Expert in at least one of USCYBERCOM's Lines of Operation to secure, operate, and defend the DODIN, plan and conduct DCO, and plan and conduct OCO when authorized
- Able to support the development of cyberspace operations plans, contingency plans, CONOPs, and orders

Qualifications:

- Minimum two years of experience as a Joint Operation Planner and a complete working knowledge of the JOPP, Joint Operation Planning and Execution System (JOPES), and APEX planning formats and guidance
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the Joint Professional Military Education Phase I (JPME I). The Joint Information Officer Planning Course (JIOPC), or other similar military operational planning courses, may be substituted for JPME I.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Joint Operation Planner

- Acts as a full participant and provides substantive contributions to JPGs and OPG/OPTs developing and integrating cyber capabilities into plans, and in support of Combatant Commander planning efforts
- Fully participates and provides substantive contributions to cyberspace operations planning activities coordination through the IJSTO to include Evaluation Request and Response Messages, SAP procedures, and the RAPCO
- Serves as a technical expert of all planning methodologies and applications in all phases of military operations, providing analytical expertise and expert knowledge of operational design,

Joint Operation Planning, and APEX

- Conducts joint operation planning in support of combat and contingency operations without supervision
- Provides technical expertise and participates in all phases and steps of the JOPP and APEX activities
- Provides significant contribution to the development of cyberspace operations plans, contingency plans, CONOPs, and orders

Qualifications:

- Minimum five years of experience as a Joint Operation Planner and a complete working knowledge of the JOPP, JOPES, and APEX planning formats and guidance
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the Joint Professional Military Education Phase II (JPME II). The JIOPC, or other similar military operation planning courses, may be substituted for JPME II.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

Four years of planning experience may be substituted with completion of an advanced Service planner school (School of Advanced Military Studies (SAMS), School of Advanced Air and Space Studies (SAASS), Joint Advanced Warfighting School (JAWS), etc.).

The Level III Cyberspace Joint Operation Planner

- Leads and acts as a full participant in JPGs and OPG/OPT developing and integrating cyber capabilities into plans, and in support of Combatant Commander planning efforts
- Coordinate cyberspace operations planning activities through the IJSTO to include Evaluation Request and Response Messages, SAP procedures, and the RAPCO
- Thinks independently and serves as an advanced technical expert of all planning methodologies and applications in all phases of military operations, providing analytical expertise and expert knowledge of operational design, Joint Operation Planning, and APEX
- Establishes joint operation planning objectives in support of combat and contingency operations without supervision
- Able to independently coordinate the development of cyberspace operations plans, contingency plans, CONOPs, and orders
- Provides extensive technical expertise; leads, and participates in all phases and steps of the JOPP and APEX activities

Qualifications:

- Minimum 10 years of experience as a Joint Operation Planner and a complete working knowledge of the JOPP, JOPES, and APEX planning formats and guidance
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the JPME II. The JIOPC, or other similar military operation planning courses, may be substituted for JPME II.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

Four years of planning experience may be substituted with completion of an advanced Service planner school (SAMS, SAASS, JAWS, etc.).

12. Cyberspace Operations Engineer Level I, II, and III

Labor Category	Description
Cyberspace Operations Engineer	<ul style="list-style-type: none">• Researches and analyzes cybersecurity capabilities to satisfy data protection requirements• Evaluates products against the customer's operational requirements• Assists with the implementation of security solutions• Researches, develops requirements, evaluates, tests, and implements new or improved information security software, devices or systems• Applies a combination of expert engineering knowledge of enterprise IT and security solutions to design, develop, and/or implement solutions to ensure they are consistent with enterprise architecture security policies• Provides planning, policy, requirements, and integration support for cyber capabilities and identifies opportunities for mission enhancement• Researches, designs, develops, and implements proof of concept data protection solutions to address vulnerabilities and assists in highly focused, quick-turnaround market research regarding technology trends and/or potential solutions to address specific requirements• Assists in the evaluation of industry offerings to identify products and technologies with the potential to support the security design, and troubleshoot and problem solve technical and non-technical issues

The Level I Cyberspace Operations Engineer

- Possesses a general technical understanding of the lifecycle of the network threats, attack vectors, and network vulnerability exploitation
- With minimal guidance, identifies gaps and overlaps across existing DODIN operations (DODIN OPS) and DCO technical capabilities
- Reports boundary protection statistics and issues to USCYBERCOM leadership
- Conducts reviews and provides comments on technical materials consisting of, but not limited to, technical documentation and reports, cyber policy and procedures, and planning materials

Qualifications:

- Minimum two years of experience as a Cyberspace Operations Engineer or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Operations Engineer

- Develops, integrates, and maintains operational TTPs and SOPs
- Recommends network management policies and procedures for implementation
- Identifies DODIN OPS and DCO enterprise management tool requirements and evaluates operational standards and tools for use
- Maintains in-depth knowledge in IT standards, protocols, and methods of exploitation
- Coordinates network defense operations with DOD Component Commands/Services/Agencies/Field Activities (CC/S/A/FAs), Intelligence Agencies, Law Enforcement (LE), and U.S. Government organizations

Qualifications:

- Minimum five years of experience as a Cyberspace Operations Engineer or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skill

The Level III Cyberspace Operations Engineer

- Applies advanced telecommunications knowledge of DOD network designs and operations to analyze and define global network centric solutions
- Analyzes and evaluates voice/video/data system solutions and provide support for joint full spectrum (terrestrial and space) system and network integration
- Conducts enterprise assessments of threats and vulnerabilities, determines deviations from

acceptable configurations and security controls, assesses the level of risk, and develops and/or recommends appropriate remediation strategies

- Maintains thorough knowledge on DODIN operations, U.S. cyberspace operations community architecture, and potential defensive capabilities for countering cyber threats
- Assesses operational risks and issues, develops effective COAs and mitigation strategies, mediates, and coordinates actions
- Analyzes and reports on technical issues of current and future DOD plans, programs, policies, and activity related to the assessment of the DODIN
- Supports the design and development of networks and associated enterprise architectures

Qualifications:

- Minimum 10 years of experience as a Cyberspace Operations Engineer or related functional area
- Minimum of Bachelor's Degree from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level III Certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

13. Cyberspace Policy Analyst Level I, II, and III

Labor Category	Description
Cyberspace Policy Analyst	<ul style="list-style-type: none"> • Conducts research, analysis, development, and coordination of strategy, policy, and doctrine for cyberspace operations at the national, DOD, Service, and Command level • Provides technical expertise on executive-level projects, analyzes, assesses, and develops future strategies, policies, and doctrines governing cyberspace operations • Supports interagency and coalition policy formulations on cyberspace issues, ensuring authorities, concerns, and equities are accurately represented • Maintains awareness of and reports significant cyber-related policy issues affecting the DOD and USCYBERCOM • Provides concise, actionable communications to senior officials, both written and orally • Performs analysis and critical thinking, assesses programmatic issues, conducts risk analysis, and proposes innovative and achievable solutions

The Level I Cyberspace Policy Analyst

- Possesses a general understanding and knowledge of existing joint cyberspace policies
- With minimal guidance, conducts research and analysis, and contributes to the development and coordination of strategy, policy, and doctrine for cyberspace operations
- Plans and prepares for interactions with researchers and policy makers and provides background support and current status for documents and presentations
- Assists with the development of reports and briefings on policy, strategy, and doctrine activities
- Assists with policy formulations on cyberspace issues and researches authorities, concerns, and equities to ensure accurate representation

Qualifications:

- Minimum five years of experience as a Cyberspace Policy Analyst or related functional area
- Minimum of Bachelor's Degree in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

- Strong analytical and problem solving skills

The Level II Cyberspace Policy Analyst

- Possesses an in-depth understanding and knowledge of existing joint cyberspace policies
- Conducts research, analysis, development, and coordination of strategy, policy, and doctrine for cyberspace operations with no guidance
- Exhibits ability to publicly present policy, doctrine, and strategy concepts in a training environment
- Plans and prepares for substantive interactions with researchers and policy makers and provides background support and current status of activities for documents and presentations
- Provides substantive content for the development of reports and briefings on policy, strategy, and doctrine activities
- Provides substantive content for policy formulations on cyberspace issues and researches authorities, concerns, and equities to ensure accurate representation

Qualifications:

- Minimum 10 years of experience as a Cyberspace Policy Analyst or related functional area
- Minimum of Bachelor's Degree in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Policy Analyst

- Independently researches, analyzes, assesses, and examines existing frameworks for DOD, interagency, national, and international cyberspace-related policy, orders, directives, doctrine, strategy, and guidance for modernization and optimization of mission efficiency and effectiveness
- Exhibits expert knowledge of the comprehensive cyberspace mission set and related topics, extending from underlying network structures, standards, and cybersecurity through operational planning and execution, and including (but not limited to) related issues such as workforce, training and development, readiness, capability development and acquisition, intelligence, authorities, legislation and regulation, partnership, and governance
- Conducts analysis of existing guidance and directive documentation to identify overlaps, gaps, and seams between policies and guidance issued by independent authorities and provides recommendations for revisions and updates, resolution, or rescission
- Identifies misaligned structures or documentation within the policy and guidance landscape,

across all levels, along with overlaps, gaps, and seams which impede or may conflict with DOD execution of the cyberspace mission set

- Proposes new logical frameworks and structures to optimize the DOD guidance landscape and to clarify linkages to interagency and national frameworks and guidance
- Acts as technical expert on executive level project teams providing technical direction, interpretation, and alternatives to exceptionally complex problems and processes relating to the subject matter
- Thinks independently and demonstrates exceptional written and oral communications skills
- Possesses a thorough and expert understanding and knowledge of existing joint cyberspace policies
- Develops reports and briefings on policy, strategy, and doctrine activities
- Performs expert analysis and critical thinking, assesses complex programmatic issues, conducts risk analysis, and proposes innovative and achievable solutions

Qualifications:

- Minimum 15 years of experience as a Cyberspace Policy Analyst or related functional area
- Minimum of Bachelor's Degree in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

14. Cyberspace Scientist Level I, II, and III

Labor Category	Description
Cyberspace Scientist	<ul style="list-style-type: none"> • Studies and provides solutions to complex cyberspace technology and operations challenges • Researches revolutionary cyber technology concepts and provides direction based on research for the development of prototypes, and test activities on innovative technologies that defend against cyberspace threats and support cyberspace operations • Designs new approaches to computing technology and provides innovative uses for existing technology, including pushing the boundaries of original intent of hardware and software • Conducts empirical evaluation of a broad spectrum of networking technologies under adverse conditions • Develops techniques that provide a means to leverage expertise and applications from alternative cyber intelligence assessment perspectives and merges them to provide a SA perspective • Provides expertise in systems and affordability/failure analysis, experimental testing, training, technical assurance oversight and evaluation of OCO capabilities, hardware design and development, and software development • Summarizes and conveys findings to technical and non-technical clients through verbal and written means

The Level I Cyberspace Scientist

- Provide technical expertise regarding custom-developed hardware or software
- Studies and provides recommendations to complex cyberspace technology and operations challenges with minimal guidance
- Possesses an in-depth understanding of OCO, DCO, and DODIN OPS and is able to identify, develop, and recommend prioritization of requirements with minimal guidance
- Leverages analytics experience and knowledge of cloud computing technologies, computer science, statistics, mathematics, and other cutting-edge technologies
- Conducts research with minimal guidance and provides recommendations for the development of innovative technologies and test activities that defend against cyberspace threats

Qualifications:

- Minimum five years of experience as a Cyberspace Scientist
- Minimum of Ph.D. from an accredited college or University in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Scientist

- Possesses a thorough understanding of OCO, DCO and DODIN OPS and is able to identify, develop, and recommend prioritization of requirements with no guidance
- Leverages in-depth analytics experience and knowledge of cloud computing technologies, computer science, statistics, mathematics, and other cutting-edge technologies
- Conducts research with no guidance and designs solutions for the development of innovative technologies and test activities that defend against cyberspace threats

Qualifications:

- Minimum 10 years of experience as a Cyberspace Scientist
- Minimum of Ph.D. from an accredited college or University in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Scientist

- Possesses an advanced understanding of OCO, DCO, and DODIN OPS and is able to identify, develop, and recommend prioritization of requirements
- Leverages advanced analytics experience and knowledge of cloud computing technologies, computer science, statistics, mathematics, and other cutting-edge technologies
- Conducts research and designs solutions and plans for the development of innovative technologies and test activities that defend against cyberspace threats

Qualifications:

- Minimum 15 years of experience as a Cyberspace Scientist
- Minimum of Ph.D. from an accredited college or University in Computer Science, Cybersecurity, Computer Engineering, or related discipline

- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

15. Cyberspace Training Facilitator Level I, II, and III

Labor Category	Description
Cyberspace Training Facilitator	<ul style="list-style-type: none"> Plans, develops, evaluates, and updates training programs, course content and materials Implements methodologies to improve the instructional design process Develops training objectives and implements methodologies to assess student progress towards meeting the training objectives Integrates course curriculums Assists in preparing instructors and ensuring instructor familiarity with the course content and objectives for delivery in classroom settings; maintains same familiarity and assists in delivery of course content

The Level I Cyberspace Training Facilitator

- With minimal guidance, designs, develops and implements training programs
- Provides input to training strategies, methodologies, and tools
- Maintains SA of technology evolution, analyzes technology evolutions, and develops associated training requirements and curriculum
- Assesses training effectiveness
- Possesses an understanding of DCO and OCO concepts
- Demonstrates an understanding of the Instructional System Development Methodology
- Possesses the ability to work efficiently in a military staff environment requiring coordination across USCYBERCOM Directorates, JFHQs, subordinate headquarters, Service Cyber components, Combatant Commands (CCMDs), components and agencies, and USCYBERCOM Strategic partners and stakeholders

Qualifications:

- Minimum two years of training experience in a cyberspace environment
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Training Facilitator

- With no guidance, designs, develops, and implements training programs
- Develops, prepares, explains, briefs, and coordinates plans, schedules, and reports
- Possesses strong writing, briefing, coaching, and leading skills

Qualifications:

- Minimum five years of training experience
- Minimum three years in a cyberspace environment
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Training Facilitator

- Customizes course content for senior military and civilian leaders
- Possesses strong writing, briefing, and teaching skills
- Possess the ability and experience of briefing and delivering training to senior military and civilian leaders

Qualifications:

- Minimum 10 years of training experience
- Minimum four years in a cyberspace environment
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

16. Cyberspace Training Specialist Level I, II, and III

Labor Category	Description
Cyberspace Training Specialist	<ul style="list-style-type: none"> Assesses effectiveness of training to ensure training meets objectives and joint standards Assist in evaluating training objectives Determines revisions for course materials Assesses courses for equivalency Assists in maintaining joint training standards Assists in assessing readiness for cyberspace forces for conducting cyberspace operations Participates in the planning and scheduling of training and exercise events and observation activities Develops requirements for collective training and exercise events Assists in identifying and tracking observations and lessons learned from training and exercise events both internally to USCYBERCOM and across the Joint Force for resolution Assists in assessing training initiatives, identifying shortfalls, and developing mitigation strategies

The Level I Cyberspace Training Specialist

- Contributes to the development and maintenance of joint standards for training
- Contributes content to the development of Readiness Reports
- Prepares and coordinates training plans, schedules, and reports
- Contributes to the development and maintenance of Training Curriculums, Schedules, Joint Cyber Training and Certification Standards, Training and Readiness Manual, and other training documentation and guidance
- Assists in coordination and development of Joint Mission Essential Tasks and review of joint mission essential task lists
- Assist in assessing USCYBERCOM's ability to meet the joint mission essential task list standards

Qualifications:

- Minimum two years of training experience

- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Cyberspace Training Specialist

- Contributes substantive content to the development and maintenance of joint standards for training
- Contributes substantive content to the development of Readiness Reports
- Contributes substantive content to the development and maintenance of Training Curriculums, Schedules, Joint Cyber Training and Certification Standards, Training and Readiness Manual, and other training documentation and guidance

Qualifications:

- Minimum five years of training experience
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Cyberspace Training Specialist

- Develops, prepares, explains, briefs, and coordinates plans, schedules, and reports
- Possesses strong writing, briefing, coaching, and leading skills

Qualifications:

- Minimum 10 years of Training experience
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

17. Graphic Artist Level I, II, and III

Labor Category	Description
Graphic Artist	<ul style="list-style-type: none">• Provides graphic arts development and support• Consults and advises customers' staff regarding graphic projects requiring artist input• Creates and visualizes ideas graphically for publications and Web sites• Revises subject matter for graphic presentation, selecting materials and processes and designs format• Prepares and oversees the preparation of original designs, drawings, graphs, charts, models, and exhibits for internal and external presentation and publication• Determines requirements for publication artwork, including selection of ink, paper, and type style in conjunction with publication customers• Consults with and advises customers concerning pending graphics, publications, and artwork, including cost estimates and artwork content• Plans and designs the production of graphics used in instructional aids, exhibits, and multi-image presentations• Reviews layouts, sketches, and final plans for production and evaluates artistic media• Coordinates production workflow of publications (periodicals, brochures, and manuscripts)• Possesses strong attention to detail and organizational skills• Possesses excellent communications skills

The Level I Graphic Artist

- Provides end-users with recommendations and general graphic artist support for the development of documents, briefings, and websites with minimal guidance
- Maintain records and files of historical, approved, and recommended graphics
- Plans and designs the production of graphics used in instructional aids, exhibits, and multi-image presentations

- Revises subject matter for graphic presentation, selecting materials and processes, and designs format with minimal guidance

Qualifications:

- Minimum two years of experience as a Graphic Artist
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Graphic Artist

- Provides end-users with recommendations and in-depth graphic artist support for the development of documents, briefings, and websites with no guidance
- Revises subject matter for graphic presentation, selecting materials and processes, and designs format with no guidance

Qualifications:

- Minimum five years of experience as a Graphic Artist
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Graphic Artist

- Provides end-users with recommendations and complex graphic artist support for the development of documents, briefings, and websites
- Plans and designs the production of graphics used in complex instructional aids, exhibits, and multi-image presentations

Qualifications:

- Minimum 10 years of experience as a Graphic Artist
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

18. Graphic Designer Level I, II, and III

Labor Category	Description
Graphic Designer	<ul style="list-style-type: none">• Designs and develops graphics and illustrations for use in technical materials, manuals, and publications• Creates, plans, designs, and prepares graphics design products, computer-generated animation, photographs, text, and abstract illustrations• Provide advice and assistance with interpreting and applying guidelines and standards for design, graphics, composition, and techniques related to the communication of information• Formulates concept and creates illustrations and detail from models, sketches, memory, written or verbal instructions, and imagination• Selects type, draws lettering, and lays out material• Determines style, technique, and medium best suited to produce desired effects and conform to reproduction requirements• Sets priorities, goals, and deadlines, and makes recommendations on how to plan and accomplish assignments that require integration and synthesis of a number of unrelated disciplines and disparate concepts

The Level I Graphic Designer

- Designs and develops graphics and illustrations for use in technical materials, manuals, and publications with minimal guidance
- Maintain records and files of historical, approved, and recommended graphics
- Understands basic concepts of cyberspace, OCO, and DCO and uses this knowledge to recommend graphic designs to communicate information pictorially

Qualifications:

- Minimum two years of experience as a Graphic Designer
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Graphic Designer

- Designs and develops substantive graphics and illustrations for use in technical materials,

manuals, and publications with no guidance

- With minimal guidance, sets priorities, goals, and deadlines, and makes recommendations on how to plan and accomplish in-depth, non-routine, and ambiguous assignments that require integration and synthesis of a number of unrelated disciplines and disparate concepts

Qualifications:

- Minimum five years of experience as a Graphic Designer
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Graphic Designer

- Designs and develops extremely complex graphics and illustrations for use in technical materials, manuals, and publications
- Operates independently, sets priorities, goals, and deadlines, and makes final recommendations on how to plan and accomplish highly complex, non-routine, and ambiguous assignments that normally require integration and synthesis of a number of unrelated disciplines and disparate concepts

Qualifications:

- Minimum 10 years of experience as a Graphic Designer
- Minimum of Bachelor's Degree in in Graphic Design, Art, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

19. Information Technology Specialist Level I, II, and III

Labor Category	Description
Information Technology Specialist	<ul style="list-style-type: none"> • Identifies user requirements and describes services available or refers inquiries to other staff • Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility • Assists in preparing documentation of supported products for users • Assists in preparing user training materials and conducts training sessions as assigned • Performs programming tasks of limited scope to assist users • Applies knowledge of computer science principles, information management principles, data processing functions, and Automated Data Processing (ADP) hardware and software systems structures and operations, and computer programming languages and techniques to solve automation problems • Addresses scientific engineering or business objectives by writing, modifying, or adapting computer programs in machine level, assembly, and third or fourth generation programming languages • Interfaces with and uses minicomputer and main computer systems in addressing project objectives • Identifies and uses standard, unconventional, and original mathematical, algorithmic, and programmatic approaches to define, plan, organize, design, develop, modify, test, and integrate database or data processing systems, computer hardware systems, and simulation models • Formulates architectural designs, functional specifications, interfaces, and documentation or hardware or software systems, considering system interrelationships, operating modes, and software or equipment configurations • Develops design specifications by inspection and analysis to offset various malware and to protect and defend USCYBERCOM infrastructure • Researches unconventional application of software and operating systems in designing and developing new methodologies, significant

modifications, or adaptations of standardized techniques

- Develops project plans, guidelines, and controls

The Level I Information Technology Specialist

- Performs entry-level IT administration and functions such as, user adds, moves and deletes, backup and restore, preventive maintenance, and upgrades
- Assists with the planning and coordination of software and applications upgrades, and Hypertext Markup Language (HTML) and Web development
- Installs, upgrades, and configures personal computers and peripherals including modems, printers, disk drives, memory and other system boards, keyboards, and monitors
- Provides initial assessment, research, and resolution of basic incidents and requests regarding the use of application software products and infrastructure components
- Addresses and resolves basic incidents and requests and logs all incidents and requests
- Designs architectures to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces
- Ensures systems are compatible and in compliance with the standards for open systems and DOD architectures
- Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture
- Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades
- Interacts with project management to plan project schedules and technical direction
- Develops software design documents and technology white papers
- Provides recommendations during the selection of development tools
- Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer
- Creates a positive client support experience and builds relationships through deep problem understanding, ensuring timely resolution
- Monitors systems and peripheral equipment, system processing, and error listings to maintain control of hardware and software malfunctions
- Responds to trouble calls, analyzes problems with software and hardware, and takes appropriate action to correct problems

- Assists users with computers, network, and application-related issues and may provide training in areas such as database, security, and LAN administration

Qualifications:

- Minimum two years of experience as an IT Specialist
- Minimum of Bachelor's Degree in Information Systems, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Information Technology Specialist

- Conducts individual and group training sessions and demonstrates how to use computer programs
- Develops, prepares, and evaluates training program outlines, training manuals, instructions, reference manuals, and other materials
- Provides training related to computerized applications
- Supports older technology during transition phases and tests new equipment, software, and technologies for replacement
- Monitors and distributes helpdesk calls and assists with report programming
- Possesses expert-level knowledge of computers and peripheral equipment, including operating systems and basic operations functions, system and memory configurations, and software
- Develops high-level system design diagrams, program design, coding, testing, debugging and documentation
- Conducts quality assurance reviews and the evaluation of existing and new software products
- Installs, operates, configures, diagnoses, and repairs computers, related software, and peripheral equipment
- Monitors activity and components of data communications networks and identifies software and hardware malfunctions
- Determines users' needs and problems, understands program requirements, and develops effective solutions; prepares documentation materials
- Presents technical concepts and procedures on software
- Establishes rapport quickly and effectively with groups and individuals and maintains effective working relationships

Qualifications:

- Minimum five years of experience as an IT Specialist
- Minimum of Bachelor's Degree in Information Systems, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Information Technology Specialist

- Possesses demonstrated expert-level experience in planning and managing large-scale upgrades, planning and scheduling large-scale migration activities, designing, installing, configuring, operating LANs and WANs, and providing expert administrative skills to solve challenging IT issues
- Effectively communicates, coordinates efforts, and establishes customer relations
- Provides top-level technical expertise, including performing in-depth and complex software systems programming and analysis
- Creates detailed design specifications for use by software development staff members

Qualifications:

- Minimum 10 years of experience as an IT Specialist
- Minimum of Bachelor's Degree in Information Systems, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum DOD 8140/DOD 8570 IAT Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

20. Inspector General Specialist Level I, II, and III

Labor Category	Description
Inspector General Specialist	<ul style="list-style-type: none"> Assists the Command Inspector General (IG) in the collection of information from all sources, internal and external, that could require analysis and independent review Establishes and maintains business processes to ensure all referred issues are fully and accurately recorded Engages with members of the command or IG working groups supporting the IG and maintains records of meetings for official purposes Supports a program of audits, inspections, and analyses to examine the actions and operations of command personnel Maintains comprehensive case logs of all cases assigned and completed, ensuring timely progress on all assigned analyses Possesses strong writing, research, and analytical skills, as well as oral communication skills, and the ability to work independently

The Level I Inspector General Specialist

- Exhibits a general understanding of the DOD and Federal Government regulations governing the conduct of the Command's cyberspace mission
- With minimal guidance, assists the Command IG in the collection of information from all sources, internal and external, that could require analysis and independent review
- With minimal guidance, establishes and maintains business processes to ensure all referred issues are fully and accurately recorded

Qualifications:

- Minimum two years of DOD IG experience
- Minimum of Bachelor's Degree in Business, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Inspector General Specialist

- Exhibits an in-depth understanding of the DOD and Federal Government regulations governing the conduct of the Command's cyberspace mission

- With no guidance, assists the Command IG in the collection of information from all sources, internal and external, that could require analysis and independent review
- With no guidance, establishes and maintains business processes to ensure all referred issues are fully and accurately recorded

Qualifications:

- Minimum five years of DOD IG experience
- Minimum of Bachelor's Degree in Business, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Inspector General Specialist

- Exhibits thorough level of understanding of the DOD and Federal Government regulations governing the conduct of the Command's cyberspace mission

Qualifications:

- Minimum 10 years of DOD IG experience
- Minimum of Bachelor's Degree in Business, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

21. Intelligence Planner Level I, II, and III

Labor Category	Description
Intelligence Planner	<ul style="list-style-type: none"> Responsible for developing, reviewing, and coordinating Command Operational Plans (OPLANs) and Concept Plans (CONPLANs), primarily Annex B (Intelligence) and the creation of Intelligence Task List (ITLs) Provides technical expertise in intelligence plans to support the Command Director of Intelligence Plans, organizes, develops, coordinates, and assists in the execution of intelligence planning activities in order to drive objectives and evaluations of intelligence planning efforts and inter-agency information sharing efforts Coordinates among operators, managers, and planners to accomplish planning tasks and provides recommendations on planning issues Promotes interchange of information requirements, capabilities, deficiencies, and technology applications in the area of specialization

The Level I Intelligence Planner

- Assists in the execution of plans in the context of combatant commands' priority intelligence planning efforts
- Supports Command with specific emphasis on control, communications, computers, intelligence, surveillance, and operations, planning, and training
- Prepares and coordinates plans, schedules, directives, and reports

Qualifications:

- Minimum two years of combined experience in intelligence planning and intelligence analysis
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the JPME I. JIOPC, or other similar military operational planning courses, may be substituted for JPME I.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

Two additional years of experience may be substituted for a Bachelor's Degree

The Level II Intelligence Planner

- Assists in coordinating efforts for the execution of plans in the context of CCMDs' priority intelligence planning effort

Qualifications:

- Minimum five years of combined experience in intelligence planning and intelligence analysis
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the JPME II. JIOPC, or other similar military operational planning courses, may be substituted for JPME II.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

Two years of intelligence planning experience may be substituted with completion of an advanced Service planner school (SAMS, SAASS, JAWS, etc.).

The Level III Intelligence Planner s

- Develops, prepares, explains, briefs, and coordinates plans, schedules, directives, and reports
- Possesses strong writing, briefing, coaching, and leading skills
- Demonstrates proven experience in military planning and joint operations with major Command staff activities
- Understands intelligence collection capabilities/planning as well as analytical procedures

Qualifications:

- Minimum 10 years of combined experience in intelligence planning and intelligence analysis
- Minimum of Bachelor's Degree from an accredited college or university
- Minimum specialized education in military joint operation planning through the JPME II. The JIOPC, or other similar military operation planning courses, may be substituted for JPME II.
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

Three years of experience may be substituted with completion of an advanced Service planner school (SAMS, SAASS, JAWS, etc.).

22. Knowledge Management Specialist Level I, II, and III

Labor Category	Description
Knowledge Management Specialist	<ul style="list-style-type: none">Conducts activities related to the knowledge management processes, to include, but not limited to: content analysis, document management, data capture, portals, shared storage locations, workflow, collaboration, data warehousing, decision support, and information dissemination; planning to encompass the strategy, architecture and methodology for an enterprise modernization effort; selection, implementation, and measure of packaged solutions for enterprise modernization; and complete integration of applications with target data and defined processes

The Level I Knowledge Management Specialist

- Utilizes knowledge building, knowledge sharing, and knowledge management skills to promote a sharing and learning culture
- Coordinates efforts to mainstream knowledge management into core USCYBERCOM activities and projects, independently builds partnerships and promotes initiatives to identify, and creates and shares knowledge relevant to solving issues and maximizing opportunities
- Promotes collaborative tools to facilitate sharing of ideas and work among internal teams and external partners
- Utilizes tools and processes to establish and nurture communities of practice including workshops, one-on-one guidance, and troubleshooting
- Maintains general knowledge, as well as practical experience, of knowledge management concepts and tools including software applications and IT systems

Qualifications:

- Minimum two years of experience as a Knowledge Management Specialist
- Minimum of Bachelor's Degree in Information Management or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Knowledge Management Specialist

- Integrates information from departments and functions throughout the organization to facilitate easy access, sharing, and dissemination of information with internal business partners and external customers
- Trains and educates front-end users of the knowledge management tools

- Develops reports as required to support operations, write knowledge content as required, and prepare presentations for senior management to support recommended changes, new initiatives or enhancements
- Monitors solution benefits and key measures of success to ensure that ongoing benefits are realized, and facilitates development of controls with business partners through streamlining processes and system automation
- Supports all positions with appropriate analysis and backup materials; collaborates across many business units to communicate complex concepts

Qualifications:

- Minimum five years of experience as a Knowledge Management Specialist
- Minimum of Bachelor's Degree in Information Management, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Knowledge Management Specialist

- Coordinates process improvement initiatives through the disciplined use of technology solutions, facilitates discussion of process alternatives in order to arrive at best practices, and coordinates the development and modification of new and existing content
- Provides operational support to USCYBERCOM by conducting and overseeing data analysis in order to optimize search results and ensure proper categorization of content within USCYBERCOM
- Provides strategic direction to business groups through initiative prioritization, integration, and resource application and ensures that policies and procedures align with the USCYBERCOM mission
- Manages content that integrates information from departments and functions throughout the organization to facilitate easy access, sharing, and dissemination of information with internal business partners and external customers
- Acts as an SME for Knowledge Management and its reporting capabilities, manages content and workflow, and educates front-end users on the use of the Knowledge Management System
- Oversees reporting to support operations and prepares analysis and recommendations related to categorization of content and optimizing search results
- Monitors solution benefits and key measures of success to ensure that ongoing benefits are realized (e.g., improved process consistency and faster onboarding of information)
- Facilitates development of controls with business partners through streamlining processes and system automation, and prepares presentations for senior management to support recommended changes, new initiatives, or enhancements

Qualifications:

- Minimum 10 years of experience as a Knowledge Management Specialist
- Minimum of Bachelor's Degree in Information Management, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

23. Legislative Affairs Specialist Level I, II, and III

Labor Category	Description
Legislative Affairs Specialist	<ul style="list-style-type: none"> • Exhibits familiarity with legislative and regulatory documents and has a working knowledge of the legislative and regulatory process • Reviews and analyzes congressional hearing transcripts and prepares/submits Questions for the Record (QFR) and Inserts for the Record (IFR) • Acts in a proactive manner with actions focused on problem-solving and aids in implementing systems and procedures to ensure that projects and documents are kept on track and internal and external deadlines are met • Researches and writes background papers, talking points, and written and oral statements, to include providing legislative briefings to leadership • Possesses ability to work with senior military and civilian leaders • Possesses the ability to prepare leadership for testifying to Congress and meeting with members of Congress and with pertinent Congressional Committee Staff Members • Possess self-motivation with excellent communications skills and ability to work independently

The Level I Legislative Affairs Specialist

- With minimal guidance, researches and writes background papers, talking points, and written and oral statements, to include providing legislative briefings to leadership
- With minimal guidance, prepares USCYBERCOM leadership for testifying to Congress and meeting with members of Congress and with pertinent Congressional Committee Staff Members

Qualifications:

- Minimum five years of experience in the field of legislative affairs or department-level planning/execution
- Minimum of Bachelor's Degree in Political Science or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Legislative Affairs Specialist

- Exhibits in-depth understanding of legislative and regulatory documents and has an in-depth knowledge of the legislative and regulatory process
- With no guidance, researches and writes background papers, talking points, and written and oral statements, to include providing legislative briefings to leadership
- With no guidance, prepares USCYBERCOM leadership for testifying to Congress and meeting with members of Congress and with pertinent Congressional Committee Staff Members

Qualifications:

- Minimum 10 years of experience in the field of legislative affairs or department-level planning/execution
- Minimum of Bachelor's Degree in Political Science or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Legislative Affairs Specialist

- Exhibits a thorough understanding of legislative and regulatory documents and has extensive knowledge of the legislative and regulatory process

Qualifications:

- Minimum 15 years of experience in the field of legislative affairs or department-level planning/execution
- Minimum of Bachelor's Degree in Political Science or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

24. Malware Analyst Level I, II, and III

Labor Category	Description
Malware Analyst	<ul style="list-style-type: none">• Employs engineering techniques and processes to analyze software to identify vulnerabilities• Re-creates programs to rebuild something similar to it, exploits its weaknesses, or strengthens its defenses• Develops design specifications by inspection and analysis to offset various malware and to protect and defend USCYBERCOM infrastructure• Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption• Conducts vulnerability assessments/penetration tests of information systems• Ensures software standards are met; designs, develops, documents, tests, and debugs applications software and systems that contain logical and mathematical solutions• Performs in-depth detailed research of software and methodologies to build defensive and offensive technical capabilities for USCYBERCOM

The Level I Malware Analyst

- Analyzes malware, spam, phishing, or any other malicious content, and components and end-to-end systems for security at the embedded-system, mobile, host, network, and enterprise level
- Performs intrusion detection analysis and vulnerability assessment and malware research and analysis
- Understands source code, hex, binary, regular expression, data correlation, and analysis such as firewall, network flow, and system logs
- Handles incidents and responds accordingly to mitigate risks

Qualifications:

- Minimum two years of experience as a Malware Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline

- A minimum of DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Malware Analyst

- Participates in formal technical briefing and proposals
- Performs system analysis, reverse engineering, and static, dynamic, and best-practice malware analytical methodologies on Windows, Android, or UNIX-based platforms
- Has an in-depth understanding of security concepts, protocols, processes, architectures, and tools (authentication and access control technologies, intrusion detection, network traffic analysis, incident handling, media/malware analysis, etc.), malware and programming skills to include C/C++ and Assembly language, and detailed understanding of how network-based attacks work at the operating system and/or protocol level

Qualifications:

- Minimum five years of experience as a Malware Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- A minimum of DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Malware Analyst

- Possesses senior-level experience as a Malware Analyst with a background in cutting-edge cyberspace technologies
- Often and without source code or documentation, performs system analysis, reverse engineering, and static, dynamic, and best-practice malware analytics methodologies and analysis on Windows, Android, or UNIX-based platforms
- Coordinates effort to develop and analyze cyberspace operations, DCO, Computer Network Exploitation (CNE), and OCO solutions
- Creates malware detection topologies
- Possesses comprehensive knowledge of programming skills especially including C/C++ and Assembly language, Windows internal C/C++ and either UNIX/Linux or mobile (Android) platform, malware and things related to malware research and analysis, reverse engineering, vulnerability analysis, exploit development, and related disciplines

Qualifications:

- Minimum 10 years of experience as a Malware Analyst

- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum of DOD 8140/DOD 8570 IASAE Level II or Computer Network Defense (CND) Certification, DOD 8140/8570 CNDSP Analyst/Infrastructure Support/Incident Responder certified.
- Strong attention to detail and organizational skills. Excellent communications skills.

25. Modeling & Simulation Engineer Level I, II, and III

Labor Category	Description
Modeling & Simulation Engineer	<ul style="list-style-type: none"> • Provides modeling and simulation functions or operations such as, but not limited to, exercises, plans, coordination, demonstrations, and instruction • Designs seminar, war games, and cyber exercise scenarios, and actively participates to assess the effectiveness of USCYBERCOM existing capabilities as well as new concepts, methods, and tools • Develops and employs modeling and simulation decision support tools to map and analyze resource planning and policy decisions by participants during war game events on future cyberspace capabilities and tools • Identifies and modifies existing modeling and simulations tools to meet war game analytical objectives and support model-run analysis during the events and post-execution

The Level I Modeling & Simulation Engineer

- With minimal guidance, conducts modeling and simulation functions or operations such as, but not limited to, exercises, plans, coordination, demonstrations, and instruction
- Contributes content to design seminars, war games, and cyber exercise scenarios, and assists in assessing the effectiveness of USCYBERCOM existing capabilities as well as new concepts, methods, and tools
- With minimal guidance, develops and employs modeling and simulation decision support tools

Qualifications:

- Minimum five years of experience as a Modeling & Simulation Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Modeling & Simulation Engineer

- With no guidance, conducts modeling and simulation functions or operations such as, but not limited to, exercises, plans, coordination, demonstrations, and instruction
- Contribute substantive content to design seminars, war games and cyber exercise scenarios, and actively participates to assess the effectiveness of USCYBERCOM existing capabilities as well

as new concepts, methods, and tools

- With no guidance, develops and employs modeling and simulation decision support tools

Qualifications:

- Minimum 10 years of experience as a Modeling & Simulation Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Modeling & Simulation Engineer

- Assists in leading modeling and simulation functions or operations such as, but not limited to, exercises, plans, coordination, demonstrations, and instruction
- Assist in leading activities to design seminar, war games, and cyber exercise scenarios, and to assess the effectiveness of USCYBERCOM existing capabilities as well as new concepts, methods, and tools
- Develops and employs complex modeling and simulation decision support tools

Qualifications:

- Minimum 15 years of experience as a Modeling & Simulation Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

26. Network Engineer Level I, II, and III

Labor Category	Description
Network Engineer	<ul style="list-style-type: none"> • Determines user requirements and design specifications for networks • Monitors networks to ensure network availability to system users • Performs necessary maintenance to support network availability • Plans, schedules, and conducts the installation of new or modified hardware and associated operating systems and software applications • Designs and conducts tests and evaluations of USCYBERCOM's networks. Analyzes and organizes the corresponding hardware and software combined solutions through network modeling and planning. • Performs system-level design and configuration of products, including determination of hardware, operating system, and other platform specifications • Evaluates new network technologies and makes recommendations to project managers regarding integration of these technologies into the existing network • Plans new network configurations and integration into existing networks to maintain optimal performance • Provides subject matter expertise to achieve joint full spectrum (terrestrial and space) network interoperability and integration

The Level I Network Engineer

- With minimal guidance, designs, proposes, and implements solutions, including writing recommendations and specifying equipment
- Provides technical assistance for the coordination of installation, upgrades, or deployment projects, including on-site direction for additional network engineers
- Assists in troubleshooting difficult or time-sensitive problems
- Provides unique area of expertise when communicating the benefits of specific technologies
- Contributes to USCYBERCOM mission and direction in helping improve technical practices
- Configures, installs, and troubleshoots centralized network infrastructure such as routers, hubs, switches, etc.

Qualifications:

- Minimum two years of experience as a Network Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum of DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Network Engineer

- Applies Network Engineering principles, methods, and tools for integrating components (for example, network equipment, protocols, telephony) to develop a functional system or prototype to test the security of computer networks
- With no guidance, deploys, configures, improves, and supports scalable production and corporate network infrastructure following enterprise best practices
- Possesses an in-depth understanding of Network Infrastructure Design as it relates to the architecture/topology of software/hardware/networks, including LANS/WANS, their components and associated protocols and standards, and how they integrate with one another
- Performs data/information management in coordination with other team members

Qualifications:

- Minimum five years of experience as a Network Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum of DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Network Engineer

- Provides technical leadership and manages the short- and long-term needs of USCYBERCOM networks, and supports projects requiring network resources and development of network-related policies and procedures
- Analyzes, identifies, and resolves network operational issues to ensure optimum performance and network capacity, and assists with the support of all server platforms that communicate through the network to determine requirements for new and existing systems
- Evaluates and selects IT services, application software, and hardware products and coordinates project teams using effective work planning and oversight practices
- Provides recommendations on current and pertinent technology; identifies and recommends

strategic directions based on technical changes in the computer industry

- Manages networks configuration involving at least several hundred locations with primary and backup connectivity and a range of connectivity types
- Designs, implements, troubleshoots, and monitors network security mechanisms to mitigate risks of network attacks
- Applies network engineering, operations, architecture, and sound management practices to manage technical staff to meet projects schedules

Qualifications:

- Minimum 10 years of experience as a Network Engineer
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Minimum of DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

27. Open Source Analyst Level I, II, and III

Labor Category	Description
Open Source Analyst	<ul style="list-style-type: none">• Collects and analyzes foreign- and domestic-based publicly available information to identify trends, patterns, and relationships that provide unique insights into cyber security issues• Provides insight into emerging cyber threats and tactics used to breach secure DOD IT infrastructure and publicly-traded United States US and international corporations• Researches and evaluates currently available and/or emerging best practices to best mitigate cyber risks• Collaborates closely with experts in cyber disciplines/specialties to perform advanced research, analysis, and fusion of information from a variety of sources to prepare a multi-layered analysis/product to support assigned projects

The Level I Open Source Analyst

- With minimal guidance, conducts open source research and analysis and develops assessments and reports
- Demonstrates a general understanding of strategy, policy, and doctrine for intelligence and cyberspace operations
- Possesses a general understanding of OCO, DCO, and DODIN Operations and is able to identify, develop, and recommend prioritization of requirements

Qualifications:

- Minimum two years of experience as an Open Source Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Open Source Analyst

- With no guidance, conducts open source research and analysis and develops assessments and reports
- Demonstrates an in-depth understanding of strategy, policy, and doctrine for intelligence and cyberspace operations
- Possesses an in-depth understanding of OCO, DCO, and DODIN Operations

Qualifications:

- Minimum five years of experience as an Open Source Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Open Source Analyst

- Conducts open source research and analysis and develops assessments and reports
- Demonstrates a thorough understanding of strategy, policy, and doctrine for intelligence and cyberspace operations
- Possesses a thorough understanding of OCO, DCO, and DODIN Operations

Qualifications:

- Minimum 10 years of experience as an Open Source Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Computer Engineering, Computer Science, Cybersecurity, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

28. Operational Design Cognitive Operator Level I, II, and III

Labor Category	Description
Operations Design Cognitive Operator	<ul style="list-style-type: none">• Proven expertise in Systems Theory or related discipline• Classroom experience training operational design techniques• Exhibits operations design knowledge and ability to associate and instruct the differences between operational design and Joint Operation Planning• Able to identify the central and prevailing problem in complex issues to coordinate the development of a viable concept design

The Level I Operational Design Cognitive Operator

- Exhibits general level of operations design knowledge and ability to associate and instruct the differences between operational design and Joint Operation Planning
- Contributes content to the conception and construction of frameworks to support operation plans and their execution
- Demonstrates a general level of critical and creative thinking, foresight, and adaptability
- Contributes to describing and structuring problems for understanding
- Contributes to the development of broad approaches to solve ill-defined problems and create desired end states

Qualifications:

- Minimum two years of post-secondary teaching experience, to include experience gained at the US Army's SAMS, Air Force SAASS, JAWS, etc., or equivalent, or through advanced Operational Art Studies Fellowship combined with a minimum of two years of Operational Design instructional experience and/or Campaign Planning/Design experience
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Operational Design Cognitive Operator

- Exhibits in-depth level of operations design knowledge and ability to associate and instruct the differences between operational design and Joint Operation Planning
- Contributes substantive content to the conception and construction of frameworks to support operation plans and their execution
- Demonstrates an in-depth level of critical and creative thinking, foresight, and adaptability

- Contributes substantive content to describe and structure problems for understanding
- Contributes substantive content to the development of broad approaches to solve ill-defined problems and create desired end states

Qualifications:

- Minimum five years of post-secondary teaching experience, to include experience gained at the US Army's SAMS, Air Force SAASS, JAWS, etc., or equivalent, or through advanced Operational Art Studies Fellowship combined with a minimum of three years of Operational Design instructional experience and/or Campaign Planning/Design experience
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.

Two years of experience may be substituted with completion of an advanced Service planner school (SAMS, SAASS, JAWS, etc.).

The Level III Operational Design Cognitive Operator

- Exhibits expert level of operations design knowledge and ability to associate and instruct the differences between operational design and Joint Operation Planning
- Assists in leading the conception and construction of frameworks to support operation plans and their execution
- Demonstrates a thorough level of critical and creative thinking, foresight, and adaptability
- Describes and structures problems for understanding
- Develops broad approaches to solve ill-defined problems and create desired end states

Qualifications:

- Minimum 10 years of post-secondary teaching experience, to include experience gained at the U.S. Army's SAMS, Air Force SAASS, JAWS, etc., or equivalent, or through advanced Operational Art Studies Fellowship combined with a minimum of three years of Operational Design instructional experience and/or Campaign Planning/Design experience
- Minimum of Bachelor's Degree from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.

Five years of experience may be substituted with completion of an advanced Service planner school (SAMS, SAASS, JAWS, etc.).

29. Operations Research Analyst Level I, II, and III

Labor Category	Description
Operations Research Analyst	<ul style="list-style-type: none"> • Provide operations research analysis support for intelligence, cyberspace operations, contingency operations, and operational-level planning, joint and multilateral training exercises, and strategic engagement policy • Analyzes actual and predictable, interacting, operational activities of systems to obtain a quantitative, rational basis for decision-making through the application of logic and scientific or economic disciplines and techniques • Devises modeling and measuring techniques, and utilizes mathematics, statistical methods, engineering methods, operational mathematics techniques (linear programming, game theory, probability theory, symbolic language, etc.) and other principles and laws of scientific and economic disciplines to investigate complex issues, identify, and solve problems, and aid better decision making • Applies and/or develops highly advanced technologies, scientific principles, theories, and concepts to assist organizations in advancing performance and operating more efficiently • Assists in addressing requirements and the evaluation of data assessment strategies: sampling, statistical analysis, evaluation, flow processing, and management assessment strategies • Develops cost-benefit analysis, data collection, data analysis, risk analysis, simulation model execution, economic analysis, and operational effectiveness studies • Delivers innovative, flexible, integrated solutions to meet changing business needs • Assists in the planning of programs and recommends technological application programs to accomplish long-range objectives

The Level I Operations Research Analyst

- Possesses a general understanding of cyberspace doctrine, policies, operations, and organizations
- Exhibits a general degree of ingenuity, creativity, and resourcefulness during the conduct of research and development and preparation of documents, briefings, and analyses which may include narrative, tabular, and graphic materials

- Interprets policies, procedures, standards, guidelines, and objectives and applies operations research principles and techniques to analytic needs
- Advises and collaborates with stakeholders to evaluate data and optimize data usage and promote information sharing
- Analyzes, reports, and develops recommendations on data related to operational metrics
- Prepares detailed assessment reports that represent data as useful information and ensure the analysis presents meaningful results
- Contributes to uncovering and resolving issues associated with the development and implementation of operational programs

Qualifications:

- Minimum five years of experience as an Operations Research Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Operations Research, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Operations Research Analyst

- Possesses an in-depth understanding of cyberspace doctrine, policies, operations, and organizations
- Exhibits an intermediate degree of ingenuity, creativity, and resourcefulness during the conduct of research and development and preparation of documents, briefings, and analyses which may include narrative, tabular, and graphic materials
- Interprets policies, procedures, standards, guidelines, and objectives and applies operations research principles and techniques to compound analytic needs
- Analyzes, reports, and develops recommendations on data related to compound operational metrics
- Substantively contributes to uncovering and resolving issues associated with the development and implementation of operational programs

Qualifications:

- Minimum 10 years of experience as an Operations Research Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Operations Research, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

- Strong analytical and problem solving skills

The Level III Operations Research Analyst

- Possesses a thorough understanding of cyberspace doctrine, policies, operations, and organizations
- Possesses the ability to work with senior military and civilian leaders
- Exhibits an exceptional degree of ingenuity, creativity, and resourcefulness during the conduct of research and development and preparation of documents, briefings, and analyses which may include narrative, tabular, and graphic materials
- Interprets policies, procedures, standards, guidelines, and objectives and applies operations research principles and techniques to complex analytic needs
- Analyzes, reports, and develops recommendations on data related to complex operational metrics
- Often acts independently to uncover and resolve issues associated with the development and implementation of operational programs

Qualifications:

- Minimum 15 years of experience as an Operations Research Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Operations Research, Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

30. Project Analyst Level I, II, and III

Labor Category	Description
Project Analyst	<ul style="list-style-type: none">• Provides support to the USCYBERCOM Program Manager to evaluate, review, monitor, and report on program performance• Conducts analysis and monitoring of program requirements, performance, schedule, and risk• Researches, collects, organizes, and interprets technical data and status relating to programs• Performs data and requirement gathering and business process analysis

The Level I Project Analyst

- With minimal guidance, assists the USCYBERCOM Program Manager with planning, initiating, monitoring, and closing out projects
- Develops and maintains relationships with program managers and the teams of USCYBERCOM-funded initiatives
- Creates, maintains, updates, and reconciles tracking and analysis documentation, spreadsheets, and information on program status and schedules
- With minimal guidance, identifies program risks and develops mitigation plans
- Assists in identifying and prioritizing requirements
- Conducts analysis on general program performance and risks, researches discrepancies, and prepares management reports and briefings
- Maintains program files in accordance with knowledge management and records management policies
- Collects data from a variety of sources and analyzes, summarizes, and incorporates data in reports
- Researches, compiles, and interprets historical program documentation
- Analyzes proposed capabilities, recommends COAs, and develops solutions to address areas of concern for shortfalls
- Organizes, prioritizes, and summarizes the content of received deliverables and materials, information, requests, and meetings
- Participates in the preparation and conduct of program reviews

Qualifications:

- Minimum two years of experience as a Project Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Project Analyst

- With no guidance, assists the USCYBERCOM Program Manager with planning, initiating, monitoring, and closing out projects
- With no guidance, identifies program risks and develops mitigation plans
- Conducts analysis on program performance and risks, researches discrepancies, and prepares management reports and briefings
- Develops and maintains management reports, implementation schedules, and key performance parameters
- Provides input and assists with requirement definition, scope of work definition, and scope management
- Participates in analysis activities, identifies actions and coordinates actions across the team
- Conducts requirements analysis, maintains record of requirements, or portions thereof, being fulfilled by projects, and dependency on other efforts

Qualifications:

- Minimum five years of experience as a Project Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills
- Desired: Certified Associate in Project Management (CAPM), Project Management Professional (PMP), or equivalent certification

The Level III Project Analyst

- Initiates action to assist the USCYBERCOM Program Manager with planning, initiating,

monitoring and closing out multiple, complex projects and deliverables

- Coordinates activities to identify program risks and develops mitigation plans
- Conducts analysis on complex program performance and risks, researches discrepancies, and prepares management reports and briefings
- Provides expertise to improve business strategy, internal processes, and program performance

Qualifications:

- Minimum 10 years of experience as a Project Analyst
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Minimum CAPM, PMP, or equivalent certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

31. Program Manager Level I, II, and III

Labor Category	Description
Program Manager	<ul style="list-style-type: none"> • Provides overall strategic management, defines the program scope and objectives, and manages program scope, schedule, budget, and risk • Develops program management plans, program documentation, work breakdown structures, program schedules, integrated master schedules, financial reports, and risk management documentation. Prepares charts, tables, graphs, and diagrams to assist in analyzing and effectively presenting information. • Reviews risk and risk mitigation activities of the program and proposes budgets for the same • Coordinates schedules to facilitate completion of task and contract deliverables, briefings/presentations, and program reviews • Ensures adherence to quality standards and reviews program deliverables • Interfaces with all areas affected by the program including other USCYBERCOM Directorates, Cyber National Mission Forces, Service Components, other Government organizations, end users, and IT services • Ensures compliance with all regulatory and administrative requirements imposed by the contract

The Level I Program Manager

- Responsible for all program management aspects of the development and implementation of assigned programs
- Develops detailed work plans, schedules, program estimates, resource plans, and status reports for assigned programs with minimal guidance
- Conducts program meetings and is responsible for program tracking and analysis
- Recommends and takes action to direct the analysis and solutions of problems

Qualifications:

- Minimum five years of experience as a Program Manager
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science,

Engineering, Law, Government Contracting, Finance/Accounting, or related discipline

- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Program Manager

- Defines program scope and objectives, and organizes, coordinates, and implements the program
- Provides day-to-day program direction, ensuring quality standards, program tracking, and analysis of assigned aspects of assigned program
- Provides technical and analytical guidance to program team
- As Principal Representative, provides status updates to the Government on the program

Qualifications:

- Minimum 10 years of experience as a Program Manager
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills
- Desired: CAPM, PMP, or equivalent certification

The Level III Program Manager

- Responsible for managing the program's scope, schedule, budget, and risk and developing program documentation such as program schedules, financial reports, and risk management documentation. Prepares charts, tables, graphs and diagrams to assist in analyzing and effectively presenting information.
- Reviews risk and risk mitigation activities of the program and proposes budgets for the same
- Evaluates, analyzes, and proposes operational and technical alternatives
- Reviews and provides input for Estimate-To-Complete, Funds and Man-Hour Expenditure Report, or other financial reports as appropriate to provide the status of funded programs. Reviews and evaluates program's Rough Order of Magnitude
- Schedules and assigns work to subordinates and subcontractors, monitors progress, and resolves discrepancies to ensure compliance with work quality standards and contract and TO requirements

- Directs technical teams and facilitates the integration of subtasks to ensure the optimal use of assigned resources and subcontractors
- Serves as focal point to the Government Program Manager for managing all tasks and subtasks and as Principal Representative for program direction and providing program status updates, including financial status
- Provides information to the Government regarding significant issues, provides recommended solutions in a transparent manner, and takes corrective action to issues brought by the Government Program Manager or Contracting Officer's Representative (COR)

Qualifications:

- Minimum 15 years of experience as a Program Manager
- Minimum of Bachelor's Degree from an accredited college or university in Program Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Minimum CAPM, PMP, or equivalent certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

32. Project Manager Level I, II, and III

Labor Category	Description
Project Manager	<ul style="list-style-type: none"> • Provides overall strategic management, defines the program scope and objectives, manages project's scope, schedule, budget, and risk • Develops project management plans, project documentation, work breakdown structures, project schedules, integrated master schedules, financial reports, and risk management documentation. Prepares charts, tables, graphs, and diagrams to assist in analyzing and effectively presenting information. • Reviews risk and risk mitigation activities of the project and proposes budgets for the same • Coordinates schedules to facilitate completion of task and contract deliverables, briefings/presentations, and project reviews • Ensures adherence to quality standards and reviews project deliverables • Interfaces with all areas affected by the project including other USCYBERCOM Directorates, Cyber National Mission Forces, Service Components, other Government organizations, end users, and IT services • Ensures compliance with all regulatory and administrative requirements imposed by the contract

The Level I Project Manager

- Responsible for all project management aspects of the development and implementation of assigned projects
- Develops detailed work plans, schedules, project estimates, resource plans, and status reports for assigned projects with minimal guidance
- Conducts project meetings and is responsible for project tracking and analysis
- Recommends and takes action to direct the analysis and solutions of problems

Qualifications:

- Minimum five years of experience as a Project Manager
- Minimum of Bachelor's Degree from an accredited college or university in Project Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline

- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Project Manager

- Defines project scope and objectives, and organizes, coordinates, and implements the project
- Provides day-to-day project direction, ensuring quality standards, project tracking, and analysis of assigned aspects of assigned project
- Provides technical and analytical guidance to project team
- As Principal Representative, provides status updates to the Government on the project

Qualifications:

- Minimum 10 years of experience as a Project Manager
- Minimum of Bachelor's Degree from an accredited college or university in Project Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills
- Desired: CAPM, PMP, or equivalent certification

The Level III Project Manager

- Responsible for managing the project's scope, schedule, budget, and risk and developing project documentation such as, project schedules, financial reports, and risk management documentation. Prepares charts, tables, graphs and diagrams to assist in analyzing and effectively presenting information.
- Reviews risk and risk mitigation activities of the project and proposes budgets for the same
- Evaluates, analyzes, and proposes operational and technical alternatives
- Reviews and provides input for Estimate-To-Complete, Funds and Man-Hour Expenditure Report, or other financial reports as appropriate to provide the status of funded projects. Reviews and evaluates projects Rough Order of Magnitude
- Schedules and assigns work to subordinates and subcontractors, monitors progress, and resolves discrepancies to ensure compliance with work quality standards and contract and TO requirements
- Directs technical teams and facilitates the integration of subtasks to ensure the optimal use of

assigned resources and subcontractors

- Serves as focal point to the Government Project Manager for managing all tasks and subtasks and as Principal Representative for project direction and providing project status updates, including financial status
- Provides information to the Government regarding significant issues, provides recommended solutions in a transparent manner, and takes corrective action to issues brought by the Government Project Manager or COR

Qualifications:

- Minimum 15 years of experience as a Project Manager
- Minimum of Bachelor's Degree from an accredited college or university in Project Management, Business Management, Economics, Political Science, Computer Science, Engineering, Law, Government Contracting, Finance/Accounting, or related discipline
- Minimum CAPM, PMP, or equivalent certification
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

33. Public Affairs Specialist Level I, II, and III

Labor Category	Description
Public Affairs Specialist	<ul style="list-style-type: none"> • Supports the planning and implementation of a comprehensive public affairs program for the Command • Coordinates efforts to inform interested public, to include other agencies, organizations, and Command personnel • Writes, edits, and prepares news release and programs for press, radio, and television as well as the organization and layout of publications and other informational material used in the public affairs program, ensuring conformation to Command and Government guidelines • Prepares responses to information requests on assigned programs from the news media, specialized groups, and/or general public; local, state, and Federal elected officials; and special interest groups, community, and civic organizations • Exhibits knowledge and application of a wide range of oral, written, social, visual communications concepts, principles, policies, practices, methods, applications, techniques, standards, and trends • Exhibits strong communication skills and ability to work independently without supervision and in a collaborative group

The Level I Public Affairs Specialist

- Contributes to the planning and implementation of a comprehensive public affairs program for the Command
- With minimal guidance, coordinates efforts to inform interested public, to include other agencies, organizations, and Command personnel
- With minimal guidance, writes, edits, and prepares information for release to the media, specialized groups, general public, Government officials, and other Government organizations
- Exhibits general knowledge and application of a wide range of oral, written, social, visual communications concepts, principles, policies, practices, methods, applications, techniques, standards, and trends

Qualifications:

- Minimum three years of experience as a DOD Public Affairs Specialist
- Minimum of High School Diploma

- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Public Affairs Specialist

- Contributes substantively to the planning and implementation of a comprehensive public affairs program for the Command
- With no guidance, coordinates efforts to inform interested public, to include other agencies, organizations, and Command personnel
- With no guidance, writes, edits, and prepares information for release to the media, specialized groups, general public, Government officials, and other Government organizations
- Exhibits in-depth knowledge of and application of a wide range of oral, written, social, visual communications concepts, principles, policies, practices, methods, applications, techniques, standards, and trends

Qualifications:

- Minimum six years of experience as a DOD Public Affairs Specialist
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Public Affairs Specialist

- Assists in leading efforts for the planning and implementation of a comprehensive public affairs program for the Command
- Assists in leading coordination efforts to inform interested public, to include other agencies, organizations, and Command personnel
- Writes, edit, and prepare information for release to the media, specialized groups, general public, Government officials, and other Government organizations with no guidance
- Exhibits thorough knowledge of and application of a wide range of oral, written, social, visual communications concepts, principles, policies, practices, methods, applications, techniques, standards, and trends

Qualifications:

- Minimum 10 years of experience as a DOD Public Affairs Specialist
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

34. Records Management Specialist Level I, II, and III

Labor Category	Description
Records Management Specialist	<ul style="list-style-type: none"> • Performs a variety of analytical and administrative duties involved in the development, implementation, and administration of the Command's records management program as well as the development of uniform systems and procedures for filing records and materials in various media formats • Exhibits an understanding of records management, scanning and document preservation, document management software, and the workflow management system • Sets up and maintains a filing and retrieval system • Maintains an extensive knowledge of Microsoft Word, Excel, Outlook, PowerPoint, and various database software packages • Exhibits the ability to organize, prioritize, manage, and carry out duties efficiently and within established timeframes • Strong communication skills and ability to work independently without supervision and in a collaborative group • Exhibits working knowledge of administering an electronic document management system in SharePoint

The Level I Records Management Specialist

- Exhibits a general understanding of the DOD records management program, records management instructions, regulations, policies, directives, and procedures
- Contributes content to the development and implementation of records management procedures and policies
- Contributes content to briefings and delivers records management briefings to groups to inform Command personal on record management policies and procedures
- With minimal guidance, performs a variety of analytical and administrative duties involved in the development, implementation, and administration of the Command's records management program

Qualifications:

- Minimum three years of experience as a Records Management Specialist
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Records Management Specialist

- Exhibits an in-depth understanding of the DOD records management program, records management instructions, regulations, policies, directives, and procedures
- Contributes substantive content to the development and implementation of records management procedures and policies
- Contributes substantive content to briefings and delivers records management briefings to groups to inform Command personal on record management policies and procedures
- With no guidance, performs a variety of analytical and administrative duties involved in the development, implementation, and administration of the Command's records management program

Qualifications:

- Minimum six years of experience as a Records Management Specialist
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Records Management Specialist

- Exhibits a thorough understanding of the DOD records management program, records management instructions, regulations, policies, directives, and procedures
- Develops briefings and delivers records management briefings to groups to inform Command personal on record management policies and procedures
- Initiates action to accomplish a variety of analytical and administrative duties involved in the development, implementation, and administration of the Command's records management program

Qualifications:

- Minimum 10 years of experience as a Records Management Specialist
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

35. SharePoint Developer Level I, II, and III

Labor Category	Description
SharePoint Developer	<ul style="list-style-type: none">• Develops, stages, tests, and hosts selected SharePoint solutions• Designs and develops web parts, InfoPath forms, Microsoft Office integration applications, workflows, page templates, branding customizations, Microsoft FAST Search for SharePoint search scopes, and web services• Creates connections to systems allowing the display of dashboards using components such as Excel, Structured Query Language (SQL) Reporting Service, etc.• Configures collaboration sites and forms authentication for staff access• Manages user access controls and security permissions for SharePoint• Assists with user acceptance testing and the preparation of user manuals and training for SharePoint applications

The Level I SharePoint Developer

- Provides technical assistance for analyzing user needs, translating them into requirements, and developing associated SharePoint solutions
- Designs and develops web parts, InfoPath forms, Microsoft Office integration applications, workflows, page templates, branding customizations, FAST search scopes, and web services with minimal guidance
- Creates connections to systems allowing the display of dashboards using components such as Excel, SQL Reporting Service, etc., with minimal guidance

Qualifications:

- Minimum three years of experience as a SharePoint Developer
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II SharePoint Developer

- Designs and develops web parts, InfoPath forms, Microsoft Office integration applications, workflows, page templates, branding customizations, FAST search scopes, and web services with no guidance

- Creates connections to systems allowing the display of dashboards using components such as Excel, SQL Reporting Service, etc., with no guidance

Qualifications:

- Minimum six years of experience as a SharePoint Developer
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III SharePoint Developer

- Designs and develops complex web parts, InfoPath forms, Microsoft Office integration applications, workflows, page templates, branding customizations, FAST search scopes, and web services

Qualifications:

- Minimum 10 years of experience as a SharePoint Developer
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

36. SIGINT Policy Analyst Level I, II, and III

Labor Category	Description
SIGINT Policy Analyst	<ul style="list-style-type: none"> Assists in the development and coordination of policies in a wide variety of forums across the IC and partners Understands all Executive Orders, DOD policies, Director of Intelligence policies, and NSA policies on the conduct and oversight of intelligence activities Assists or coordinates the implementation of an Intelligence Oversight (IO) program to include maintaining and retaining IO records, ensuring appropriate training, and acting to report substantiated allegations Consults with command legal counsel as appropriate Communicates with senior officers both written and orally Provides advice and guidance on SIGINT and IO policy issues to senior level management and validates the alignment of draft policies with USCYBERCOM, IC, and DOD interests

The Level I SIGINT Policy Analyst

- Demonstrates a general understanding of SIGINT and IO policies and programs
- Understands all Executive Orders, DOD policies, Director of Intelligence policies, and NSA policies on the conduct and oversight of intelligence activities at a general technical level
- Contributes to the development and coordination of policies in a wide variety of forums across the IC and partners

Qualifications:

- Minimum five years of experience in SIGINT with a minimum of three of the five years in IO and SIGINT policy experience
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II SIGINT Policy Analyst

- Demonstrates an in-depth understanding of SIGINT and IO policies and programs

- Understands all Executive Orders, DOD policies, Director of Intelligence policies, and NSA policies on the conduct and oversight of intelligence activities at an intermediate technical level
- Contributes substantive content for the development and coordination of policies in a wide variety of forums across the IC and partners

Qualifications:

- Minimum 10 years of experience in SIGINT with a minimum of four of the 10 years in IO and SIGINT policy experience
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III SIGINT Policy Analyst

- Demonstrates a thorough understanding of SIGINT and IO policies and programs
- Understands all Executive Orders, DOD policies, Director of Intelligence policies, and NSA policies on the conduct and oversight of intelligence activities at a technical expert level
- Assists in leading efforts for the development and coordination of policies in a wide variety of forums across the IC and partners

Qualifications:

- Minimum 15 years of experience in SIGINT with a minimum of five of the 15 years in IO and SIGINT policy experience
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

37. Software Developer Level I, II, and III

Labor Category	Description
Software Developer	<ul style="list-style-type: none"> • Inspects, cleans, transforms, and models data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making • Possesses knowledge across the entire field of software technologies and engineering, including information, documentation, databases, model and architecture repositories, analysis, training, testing, data synthesis, hardware, software, standards, economic consideration of selecting techniques and processes, and interoperability • Develops software planning documentation, software requirements and design documentation, software support documentation, software test description documentation, • Conducts software validation and verification, and software engineering anomaly resolution • Performs tasks in accordance with applicable DOD guidance (e.g., DOD Directive (DODD) 5000.1 and DOD Instruction (DODI) 5000.2) and industry standards (e.g., IEEE/EIA 12207.0, 12207.1, 12207.2, and ISO 9000-3) • Possesses technical knowledge and familiarity to work with the installation, demonstration, test, validation and evaluation of new and existing software, tools, methods, and software measurement technologies • Performs computer network exploitation development: embedded reverse engineering, vulnerability research, and application development for software and embedded systems with a focus on OCO, DCO, and CNE activities • Evaluates the quality of proposed and existing software systems and solutions that support various cyber software activities and are planned to be integrated into various networks and architectures • Performs needs and risk analysis of software packages [developmental Government Off-The-Shelf (GOTS) and COTS] relative to mission requirements • Develops, updates, and evaluates software engineering standards, specifications, handbooks, or manuals in relation to the development and testing of cyber capabilities • Documents verification and validation of solution sets and protocols,

and provide technical assistance to user organizations with all aspects of software acquisition

- Develops life cycle models and customizes software analytical tools, models, decision aids, screening methods, and techniques used to evaluate and support the authenticity and continuity of DOD, national, commercial, and international information systems
- Develops specialized software/firmware modules to run on embedded hardware that communicate across native communications channels and implement specialized functions on embedded systems
- Disassembles and analyzes software and embedded firmware
- Collaborates with Cyber Innovation Unit staff working multifunctional programs integrating hardware and software reverse engineering tasks
- Develops, creates, and modifies general computer applications software or specialized utility programs

The Level I Software Developer

- Provides technical assistance for analyzing user needs, translating them into requirements, and developing associated software solutions
- Coordinates and collaborates with a team of Integrators, Testers, and Network Engineers to meet criteria for each requirement
- Writes technical documentation to include, but not limited to, technical management plans, schedules, requirements documents, test documents, deployment documents, and technical briefings
- Develops code, tests, and debugs new software or enhancements to existing software.
- Provides technical support in the evaluation of software development
- Makes recommendations for improving documentation and development process standards
- Assists with developing and executing test procedures for prototype components
- Writes and reviews software and system documentation and software user manuals
- Develops research solutions by analyzing system performance standards, conferring with users or system engineers; analyzing system flow, data usage and work processes; and investigating problem areas
- Serves as research team lead at the level appropriate to the software prototype development process being used on any particular project

- Modifies existing software to correct errors, to adapt to new hardware, or to improve its performance
- Designs, develops, and modifies software systems using scientific analysis and mathematical models to predict and measure outcomes and consequences of design
- Designs or implements complex database or data repository interfaces/queries
- Supports tactical engineering activities to include participating in design meetings and technical review meetings, developing technical plans to guide capability development, preparing test plans and procedures, executing tests and writing test reports, reporting status of capability development activities, and reporting goals and results

Qualifications:

- Minimum two years of experience in application software development
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Software Developer

- Designs, develops, enhances, debugs, integrates, and implements software. Troubleshoots production problems related to software applications.
- Researches, tests, builds, and coordinates the conversion and/or integration of new products based on user requirements
- Designs or implements complex algorithms requiring adherence to strict timing, system resource, or interface constraints; performs quality control on team products
- Confers with system engineers and hardware engineers to derive requirements and to obtain information on project limitations and capabilities, performance requirements, and interfaces.
- Oversees one or more software application development teams and ensures the work is completed in accordance with constraints of the software development process being used on any particular project and deliver solutions

Qualifications:

- Minimum five years of experience in application software development
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Software Developer

- Designs, troubleshoots, and implements software code for end-to-end software development
- Coordinates project teams to develop concept, interface design, and architecture
- Researches, tests, builds, and coordinates the integration of new requirements to meet organizational needs
- Initiates action for evaluation and recommendation of application software packages, application integration and testing tools
- Resolves problems with software and responds to suggestions for improvements and enhancements
- Coordinates system installation and monitors equipment functioning to ensure operational specifications are met
- Implements recommendations for improving documentation and development process standards
- Selects the prototype development process in coordination with customer and system engineering
- Recommends new technologies and research processes for complex software development projects
- Ensures quality control of all developed and modified prototype software
- Delegates programming and testing responsibilities to one or more teams and monitors their performance
- As required, acts as an Agile process SCRUM Master
- Mentors other staff to improve reverse engineering skills

Qualifications:

- Minimum 10 years of experience in application software development
- Minimum of Bachelor's Degree in a technical discipline from an accredited college or university in Computer Science, Cybersecurity, Computer Engineering, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.

38. Special Security Officer Specialist Level I, II, and III

Labor Category	Description
Special Security Officer Specialist	<ul style="list-style-type: none">• Supports the management and oversight of a comprehensive Special Compartmented Information (SCI) program• Manages and maintains security files and forms including, but not limited to, foreign national association reports, unofficial travel requests, investigation packages, and security accreditation• Possesses excellent communication and interpersonal skills, and proficiency in Microsoft Office Suites software: Word, PowerPoint, and Excel• Exhibits knowledge of all security oversight publications, instructions, and guides• Possesses practical knowledge and experience with the Joint Personnel Adjudication System (JPAS) and Scattered-Castles

The Level I Special Security Officer Specialist

- Exhibits a basic level of knowledge of all security oversight publications, instructions, and guides
- Possesses self-motivation with strong written and oral communication skills, exceptional attention to detail, and the ability to work independently
- Possesses a general understanding of cyberspace doctrine, policies, operations, and organizations
- Contributes content to the development and implementation of security policies
- Monitors, reviews, and assists in implementing security policies, directives, and instructions

Qualifications:

- Minimum three years of experience performing Special Security Officer duties
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Special Security Officer Specialist

- Exhibits an in-depth level of knowledge of all security oversight publications, instructions, and guides.
- Contributes substantive content to the development and implementation of security policies.
- Initiates action towards accomplishing assignments and assists in furthering progress toward predetermined long-range goals and objectives

Qualifications:

- Minimum five years of experience performing Special Security Officer duties
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Special Security Officer Specialist

- Exhibits an expert level of knowledge of all security oversight publications, instructions, and guides.
- Develops draft security policies and contributes to the implementation of security policies.
- Possesses the ability to work with senior military and civilian leaders and participates at community of interest forums
- Makes and implements recommendations to ensure security compliance with policy and security guidance documents

Qualifications:

- Minimum 10 years of experience performing Special Security Officer duties
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.

39. Subject Matter Expert Level I, II, and III

Labor Category	Description
Subject Matter Expert (SME)	<ul style="list-style-type: none">• Serves as SME, possessing in-depth knowledge on subjects relating to the conduct, activities, governance, business practices, or operation of USCYBERCOM• Provides extensive technical knowledge and analysis of exceptionally complex problems that need extensive knowledge of the subject matter for effective development and implementation of solutions• Provides technical solutions to a wide range of complex problems• Works independently without supervision• Possesses understanding and has wide experience in the application of technical principles, theories, and concepts in the required technical field, and has full knowledge of other related disciplines• Provides technical expertise in a particular area of IT (e.g., Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Communications, Network Systems Management, etc.) or a specific USCYBERCOM functional area (e.g., logistics, cyberspace operations research, joint operation planning, policy, technical intelligence, etc.)

The Level I Subject Matter Expert

- Provides expert support, analysis, and research with only broad direction into exceptionally complex problems and processes relating to the subject matter
- Serves as technical expert on high-level project teams providing technical direction, interpretation, and alternatives
- Works under only general direction, thinks independently, and demonstrates superior written and oral communications skills
- Independently determines and develops approaches to solutions and develops solutions that are imaginative, thorough, practicable, and consistent with organizational objectives
- Contributes to the completion of specific programs and projects

Qualifications:

- Minimum 10 years of experience in the area of expertise
- Minimum of Bachelor's Degree in a technical or business discipline in the area of expertise from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level II Subject Matter Expert

- Guides the completion of specific programs and projects relating to the subject matter
- With no direction, provides expert support, analysis, and research into exceptionally complex problems and processes relating to the subject matter
- Serves as a technical expert on executive-level project teams providing technical direction, interpretation, and alternatives
- Thinks independently and demonstrates exceptional written and oral communication skills
- Exercises considerable latitude in determining technical objectives of assignment
- Independently develops technical solutions to complex problems that require the regular use of ingenuity and creativity
- Guides the successful completion of major programs and may function in a project leadership role

Qualifications:

- Minimum 15 years of experience in the area of expertise
- Minimum of Bachelor's Degree in a technical or business discipline in the area of expertise from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

The Level III Subject Matter Expert

- Initiates action for providing expert support, analysis, and research into exceptionally complex problems and processes relating to the subject matter
- Applies advanced technical principles, theories, and concepts on unusually complex technical problems and provides innovative and ingenious solutions
- Works under consultative direction toward predetermined long-range goals and objectives; assignments are often self-initiated
- Initiates action, determines and pursues COAs necessary to obtain desired results
- Contributes to the development of new principles and concepts
- Develops advanced technological ideas and guides their development into a final product

Qualifications:

- Minimum 20 years of experience in the area of expertise
- Minimum of Bachelor's Degree in a technical or business discipline in the area of expertise from an accredited college or university
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong analytical and problem solving skills

40. Systems Administrator Level I, II, and III

Labor Category	Description
Systems Administrator	<ul style="list-style-type: none">• Organizes and directs the configuration and operation of information management systems• Provides the day-to-day system administration to include system and resource optimization, and user assistance• Conducts capacity and performance analysis, and provides system configuration change and upgrade recommendations• Increases system administrator efficiency and accuracy via the use of automated tools and scripts, develops system administrator procedures, and conducts system administrator training and skills assessment• Determines computer user needs; analyzes system capabilities and programming techniques and controls

The Level I Systems Administrator

- Provides advice and assistance to users in accessing and using business systems
- Coordinates the daily activities of configuration and operation of business systems
- Performs system capacity analysis and planning
- Responds to users' needs in a timely manner

Qualifications:

- Minimum three years of system administrator experience
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Systems Administrator

- Manages the daily activities of configuration and operation of systems and performs system capacity analysis and planning
- Maintains servers, creates monitoring reports and logs, and ensures functionality of system links
- Monitors systems for acceptable performance and user accessibility, establishes back-ups, and

monitors systems security

- Supervises technical staff; develops and coordinates project directions and schedules to maximize benefits and minimize impacts on the customer organization
- Performs multiple tasks concurrently and responds to emergency situation effectively

Qualifications:

- Minimum six years of system administrator experience
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Systems Administrator

- Performs system capacity analysis and planning, maintains servers, creates monitoring reports and logs, and ensures functionality of system links
- Performs configuration management and documentation of network and system topologies
- Prepares technical implementation plans that provide integrated solutions, including actions, milestones, timelines, and critical paths required for complete solutions
- Possesses comprehensive knowledge of the organization's hardware, software, and network components in addition to knowledge of programming languages and operating systems, current equipment and technologies in use, enterprise backup and recovery procedures, and system performance monitoring tools
- Plans, organizes, and documents complex system design activities and configure systems to be consistent with the USCYBERCOM policies and procedures

Qualifications:

- Minimum 10 years of system administrator experience
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAT Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

41. Systems Engineer Level I, II, and III

Labor Category	Description
Systems Engineer	<ul style="list-style-type: none">• Evaluates, develops, and delivers technical input to the systems engineering process• Develops technical documentation, system architecture, and system design documentation• Interacts with the Government regarding Systems Engineering technical considerations and for associated problems, issues, or conflicts• Oversees the technical integrity of work performed and deliverables associated with the Systems Engineering area of responsibility• Communicates with other program personnel, Government overseers, and senior executives

The Level I System Engineer

- Performs requirements analysis for systems missions and environments to identify functional definitions and design for system hardware and software
- Analyzes user's requirements, develops CONOPs documents, high-level system architectures, and system requirements specifications
- Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies; provides technical leadership for the integration of requirements, design, and technology; and incorporates new plans, designs, and systems into ongoing operations
- Defines performance and design constraints and develops specifications, drawings, and product description data
- Possesses knowledge of engineering policies and procedures
- Conducts engineering research and analysis
- Organizes works to ensure tasking, projects, and assignments are completed according to deadlines
- Contributes to the development of sections of IT and telecommunications systems
- Performs system integration, system administration, or network engineering tasks

Qualifications:

- Minimum two years of experience as a System Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering

or related discipline.

- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II System Engineer

- Analyzes system requirements and coordinates design and development activities
- Conducts briefings to a variety of audiences and conveys information in a clear and articulate manner
- Performs thorough engineering analysis and quick issue resolution simultaneously
- Works both independently and as part of a team to identify problems and develop solutions in accordance with USCYBERCOM and Defense regulatory guidance
- Prioritizes and manages multiple tasks to ensure timely project completion

Qualifications:

- Minimum five years of experience as a System Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III System Engineer

- Guides system development and implementation planning through assessment or preparation of system engineering management plans and system integration and test plans
- Analyzes complex information and independently takes appropriate actions to resolve problems
- Provides engineering guidance to technical staff and establishes effective working relationships with other Government agencies and mission partners
- Delivers briefings on complex topics to groups, which may include high-level decision makers
- Works complex research projects as senior contributors and as part of an integrated research team
- Designs and delivers solutions

Qualifications:

- Minimum 10 years of experience as a System Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering

or related discipline

- Minimum DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

42. Systems Integrator Level I, II, and III

Labor Category	Description
Systems Integrator	<ul style="list-style-type: none">• Maintains integrity of systems-of-systems by defining architecture requirements (consistent with USCYBERCOM's Enterprise Architecture) and interfaces• Provides adequate and appropriate planning for end-to-end integration support throughout a system life cycle• Provides a total systems perspective including a technical understanding of relationships, dependencies, and requirements of hardware and software components• Coordinates with team members to ensure problem solution, appropriate risk reduction, and user satisfaction• Makes recommendations on test and evaluation strategies for major systems installations

The Level I Systems Integrator

- Plans, implements, tests, documents, and maintains solutions to total systems or subsystems using internally created and/or COTS products
- Prepares engineering plans and site installation technical design packages
- Coordinates the analysis, acquisition, and installation of hardware and software
- Gathers and analyzes data to support the development of system requirements
- Provides post-installation and integration support to the Government

Qualifications:

- Minimum two years of experience as a System Integrator
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Systems Integrator

- Develops work plans, procedures, and estimates as they relate to systems integration tasks and team members

- Interfaces with various team members to implement tasks according to the plans

Qualifications:

- Minimum five years of experience as a System Integrator
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Systems Integrator

- Researches, evaluates, and recommends systems/equipment/technologies to meet organizational requirements
- Develops technical instructions, engineering plans, technical designs, and other systems-integration-related documents

Qualifications:

- Minimum 10 years of experience as a System Integrator
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

43. Technical Writer Level I, II, and III

Labor Category	Description
Technical Writer	<ul style="list-style-type: none">Assists in collecting and organizing information required for preparation of documents, training materials, guides, proposals, and reportsProvides technical edits to engineering documentation, software documentation, manuals, reports, or any other documents or presentationsUtilizes strong writing, editing, and communication skills to analyze and present complex information in a format that is easy to read and understand

The Level I Technical Writer

- Works with teams to obtain a general understanding of scientific and technical information, documentation content, and requirements
- Analyzes existing and potential content and suggests enhancements to content and its presentation
- With minimal guidance, develops diagrams, charts, and graphs that increase the user's understanding
- Standardizes content across document and briefing libraries
- Develops high-quality documentation with minimal guidance that is easy-to-understand, easy to use, meets applicable standards, and meets the objectives and goals for the intended audience
- Revises documents to remain current to the projects progress

Qualifications:

- Minimum three years of experience as a Technical Writer
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong working knowledge in Microsoft Office and excellent writing skills

The Level II Technical Writer

- Works with teams to obtain an in-depth understanding of scientific and technical information, documentation content, and requirements

- With no guidance, develops diagrams, charts, and graphs that increase the user's understanding
- Develops high-quality documentation with no guidance that is easy-to-understand, easy to use, meets applicable standards, and meets the objectives and goals for the intended audience

Qualifications:

- Minimum six years of experience as a Technical Writer
- Minimum of High School Diploma
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong working knowledge in Microsoft Office and excellent writing skills

The Level III Technical Writer

- Possesses a thorough understanding of the scientific and technical subject matter, documentation content, and requirements
- Recommends and develops diagrams, charts, and graphs that increase the user's understanding

Qualifications:

- Minimum 10 years of experience as a Technical Writer
- Minimum of Bachelor's Degree or higher from an accredited college or university in English, Business, or related discipline
- Strong attention to detail and organizational skills. Excellent communications skills.
- Strong working knowledge in Microsoft Office and excellent writing skills

44. Test Engineer Level I, II, and III

Labor Category	Description
Test Engineer	<ul style="list-style-type: none"> • Performs specialized tests to support analysis and evaluation of technologies and systems • Develops test and evaluation plans and test procedures with acceptable pass rating results • Compiles and analyzes documentation, data, and other products to evaluate and validate sensor system performance capabilities and effectiveness, assesses risk, and determines operational feasibility and benefits of USCYBERCOM systems or technology prototypes to include recommending assessments of system performance, identifying deficiencies, and investigation of physical science phenomena • Conducts evaluations of the quality of proposed and existing software systems and solutions that support various cyberspace software activities to be integrated into various networks and architectures • Conducts capability vulnerability assessments and testing customized to the system function and technical requirements and based on status within security assessment and authorization cycle and authority to operate status • Evaluates capabilities components against their ability to resist threats in the deployed environment, configurations, and implementation of firewalls, proxy servers, routers, VPNs, IDS, wireless networks, etc., against legal requirements, departmental /local procedures associated with operations • Conceives, proposes, designs, and builds software projects in support of Research and Development (R&D) activities to develop cyber tools and techniques to mitigate identified vulnerabilities • Conducts highly Penetration Testing Projects, including: <ul style="list-style-type: none"> • Internal Penetration Testing (Networks, Servers, Workstations) and stealth techniques for evading Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), (IDS/IPS) • External Penetration Testing (Email, Web Services, Remote Access, etc.) • Web Application Penetration Testing (Anonymous and

	<p>Authenticated)</p> <ul style="list-style-type: none"> • Data Exfiltration Assessments • System administration in areas such as Database Security (Microsoft SQL and Oracle), Network Architecture (Cisco and Checkpoint), Mobile Device Management, Web Servers (IIS and Apache), and Virtualization
--	---

The Level I Test Engineer

- Conducts test, evaluation, and analysis activities with minimal guidance
- Provides content towards the development of test and evaluation plans and test procedures
- Tests software applications for operational deployment throughout the entire systems' life cycle
- Contributes to test and evaluation planning and preparation activities
- Contributes to the planning and development of test environments that are to be integrated into the USCYBERCOM test enterprise architecture
- Performs tests and experimentation in support of USCYBERCOM test activities/ experimentations to include test architecture development, equipment calibrations, repairs, modifications, and adjustments to support task objectives
- Analyzes capabilities for potential vulnerabilities that may result from improper system configuration, hardware or software flaws, or operational weaknesses
- Presents any security issues that are found to the system owner with an assessment of impact and a recommendation for mitigation or a technical solution
- Assesses system information security policies against client policies
- Ensures policies are comprehensive to the system

Qualifications:

- Minimum five years of experience as a Test Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Test Engineer

- Conducts test, evaluation, and analysis activities with no guidance
- Provides substantive content towards the development of test and evaluation plans and test

procedures

- Substantively contributes to the planning and development of test environments that are to be integrated into the USCYBERCOM test enterprise architecture
- Conducts prototype assessments in field environments, operates test instrumentation, and supports remote testing

Qualifications:

- Minimum 10 years of experience as a Test Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IAM Level I Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Test Engineer

- Conducts complex test, evaluation, and analysis activities
- Conducts test and evaluation planning and preparation activities
- Develops test and evaluation plans, and test procedures
- Coordinates the planning and development of test environments that are to be integrated into the USCYBERCOM test enterprise architecture
- Coordinates wargame efforts and coordinates with functional area SMEs, as needed, for facilitation, operational cyber subject matter expertise, senior policy subject matter expertise, Modeling and Simulation (M&S) development expertise, and administrative and logistics support for the wargame seminars and capstone events

Qualifications:

- Minimum 15 years of experience as a Test Engineer
- Minimum of Bachelor's Degree from an accredited college or university in System Engineering or related discipline
- Minimum DOD 8140/DOD 8570 IASAE Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

45. Web Developer Level I, II, and III

Labor Category	Description
Web Developer	<ul style="list-style-type: none">• Designs and builds web sites using a variety of graphics software applications, techniques, and tools• Designs and develops user interface features, site animation, and special effects elements• Contributes to the design group's efforts to enhance the look and feel of the organization's on-line offerings• Designs the website to support the organization's strategies and goals relative to external communications

The Level I Web Developer

- With minimal guidance, designs and builds web sites using a variety of graphics software applications, techniques, and tools
- Designs and develops basic user interface features, site animation, and special effects elements
- Contributes to the design group's efforts to enhance the look and feel of the organization's on-line offerings

Qualifications:

- Minimum three years of experience as a Web Developer
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level II Web Developer

- With no guidance, designs and builds web sites using a variety of graphics software applications, techniques, and tools
- Designs and develops substantive user interface features, site animation, and special effects elements
- Contributes substantive content to the design group's efforts to enhance the look and feel of the organization's on-line offerings

Qualifications:

- Minimum six years of experience as a Web Developer

- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

The Level III Web Developer

- Designs and builds complex web sites using a variety of graphics software applications, techniques, and tools
- Designs and develops complex user interface features, site animation, and special effects elements
- Assists in leading efforts to design and enhance the look and feel of the organization's on-line offerings

Qualifications:

- Minimum 10 years of experience as a Web Developer
- Minimum of High School Diploma
- Minimum DOD 8140/DOD 8570 IAM Level II Certification
- Strong attention to detail and organizational skills. Excellent communications skills.

ACRONYM LIST

ADP	Automated Data Processing
APEX	Adaptive Planning and Execution
BPR	Business Process Reengineering
C2	Command and Control
C&A	Certification and Accreditation
CAPM	Certified Associate in Project Management
CCB	Configuration Control Board
CCMD	Combatant Command
CC/S/A/FAs	Commands/Services/Agencies/Field Activities
CIKR	Critical Infrastructure and Key Resources
CM	Configuration Management
CND	Computer Network Defense
CNE	Computer Network Exploitation
CO	Contracting Officer
COA	Course of Action
CONOP	Concept of Operation
CONPLAN	Concept Plan
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf
C-RAP	Cyber Request and Approval
CTO	Cyber Tasking Order
DCO	Defensive Cyber Operations
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DODIN OPS	Department of Defense Information Network Operations
GOTS	Government Off-The-Shelf
HTML	Hypertext Markup Language
IAM	Information Assurance Management
IAT	Information Assurance Technical
IASAE	Information Assurance System Architect & Engineer
IC	Intelligence Community
IDIQ	Indefinite Delivery Indefinite Quantity
IDS	Intrusion Detection System
IFR	Inserts for the Record
IG	Inspector General
IJSTO	Integrated Joint Special Technical Operations
IO	Intelligence Oversight

IPS/IDPS	Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS)
iSCSI	Internet Small Computer System Interface
IT	Information Technology
ITL	Intelligence Task List
JAWS	Joint Advanced Warfighting School
JIOPC	Joint Information Officer Planning Course
JOPES	Joint Operation Planning and Execution System
JOPP	Joint Operation Planning Process
JPAS	Joint Personnel Adjudication System
JPG	Joint Planning Group
JPME I	Joint Professional Military Education Phase I
JPME II	Joint Professional Military Education Phase II
JTCB	Joint Targeting Coordination Board
JTCR	Joint Tactical Cyber Request
JTWG	Joint Targeting Working Group
LAN	Local Area Network
LCAT	Labor Category
LE	Law Enforcement
M&S	Modeling and Simulation
MCOP	Master Cyber Operations Plan
MOE	Measure of Effective
MOP	Measure of Performance
NSA	National Security Agency
OCO	Offensive Cyber Operations
OPG	Operational Planning Group
OPLAN	Operational Plan
OPT	Operational Planning Team
PMP	Project Management Professional
QFR	Questions for the Record
R&D	Research and Development
RAPCO	Review and Approval Process for Cyberspace Operations
SA	Situational Awareness
SAASS	School of Advanced Air and Space Studies
SAMS	School of Advanced Military Studies
SAP	Special Access Program
SCI	Special Compartmented Information
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SQL	Structured Query Language
STO	Special Technical Operation
TO	Task Order
TTP	Tactic, Technique, and Procedure
US	United States
USCYBERCOM	United States Cyber Command

VPN
WAN

Virtual Private Network
Wide Area Network

ATTACHMENT C -

PROBLEM NOTIFICATION REPORT

CONTRACT or TASK

ORDER NUMBER: _____ DATE: _____

1. Nature and sources of problem:
2. COTR was verbally notified on: (date) _____
3. Is action required by the Government? Yes _____ No _____
4. If YES, describe Government action required and date required:
5. Will problem impact delivery schedule? Yes _____ No _____
6. If YES, identify what deliverables will be affected and extent of delay:
7. Can required delivery be brought back on schedule? Yes _____ No _____
8. Describe corrective action needed to resolve problems:
9. When will corrective action be completed?
10. Are increased costs anticipated? Yes _____ No _____
11. Identify amount of increased costs anticipated, their nature, and define Government responsibility for problems and costs:

**NON-DISCLOSURE AGREEMENT
BETWEEN
U.S. GENERAL SERVICES ADMINISTRATION (GSA)
FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT CENTER
(FEDSIM)
AND
[CONTRACTOR]**

This agreement, made and entered into this _____ day of _____, 20XX (the "Effective Date"), is by and between GSA and [CONTRACTOR].

WHEREAS, [CONTRACTOR] and GSA FEDSIM have entered into [Contract No.], Task Order No. [INSERT] for services supporting the US CYBERCOMMAND (USCYBERCOM).

WHEREAS, [CONTRACTOR] is providing [DESCRIPTION, e.g., consulting/professional IT, engineering] services under the Task Order;

WHEREAS, the services required to support [PROGRAM/PROJECT NAME] involve certain information which the Government considers to be "Confidential Information"¹ as defined herein;

WHEREAS, GSA desires to have [CONTRACTOR]'s support to accomplish the Task Order services and, therefore, must grant access to the Confidential Information;

WHEREAS, [CONTRACTOR] through its work at a Government site may have access to Government systems or encounter information unrelated to performance of the Task Order which also is considered to be Confidential Information as defined herein;

WHEREAS, GSA on behalf of USCYBERCOM desires to protect the confidentiality and use of such Confidential Information;

NOW, THEREFORE, for and in consideration of the mutual promises contained herein, the parties agree as follows:

- 1. Definitions.** "Confidential Information" shall mean any of the following: (1) "contractor bid or proposal information" and "source selection information" as those terms are defined in 41 U.S.C. § 2101; (2) the trade secrets or proprietary information of other companies; (3) other information, whether owned or developed by the Government, that has not been previously made available to the public, such as the requirements, funding or budgeting data of the Government; and *for contracts/orders providing acquisition assistance*,

¹ This does not denote an official security classification.

this term specifically includes (4) past performance information, actual/proposed costs, overhead rates, profit, award fee determinations, contractor employee data of offerors/contractors, methods or procedures used to evaluate performance, assessments, ratings or deliberations developed in an evaluation process, the substance of any discussions or deliberations in an evaluation process, and any recommendations or decisions of the Government unless and until such decisions are publicly announced. This term is limited to unclassified information.

2. **Limitations on Disclosure.** [CONTRACTOR] agrees (and the [CONTRACTOR] Task Order personnel must agree by separate written agreement with [CONTRACTOR]) not to distribute, disclose or disseminate Confidential Information to anyone beyond the personnel identified in the [ATTACHED ADDENDUM], unless authorized in advance by the GSA Contracting Officer in writing. The Contracting Officer and Technical Point of Contact will review the Addendum to ensure it includes only those individuals to be allowed access to the information. The Addendum, which may be updated from time to time, is approved when signed by the GSA Contracting Officer and Technical Point of Contact.
3. **Agreements with Employees and Subcontractors.** [CONTRACTOR] will require its employees and any subcontractors or subcontractor employees performing services for this Task Order to sign non-disclosure agreements obligating each employee/subcontractor employee to comply with the terms of this agreement. [CONTRACTOR] shall maintain copies of each agreement on file and furnish them to the Government upon request.
4. **Statutory Restrictions Relating to Procurement Information.** [CONTRACTOR] acknowledges that certain Confidential Information may be subject to restrictions in Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. § 2104), as amended, and disclosures may result in criminal, civil, and/or administrative penalties. In addition, [CONTRACTOR] acknowledges that 18 U.S.C. § 1905, a criminal statute, bars an employee of a private sector organization from divulging certain confidential business information unless authorized by law.
5. **Limitations on Use of Confidential Information.** [CONTRACTOR] may obtain Confidential Information through performance of the Task Order orally or in writing. These disclosures or this access to information is being made upon the basis of the confidential relationship between the parties and, unless specifically authorized in accordance with this agreement, [CONTRACTOR] will:
 - a) Use such Confidential Information for the sole purpose of performing the [PROGRAM/PROJECT] support requirements detailed in the Task Order and for no other purpose;
 - b) Not make any copies of Confidential Information, in whole or in part;

- c) Promptly notify GSA in writing of any unauthorized misappropriation, disclosure, or use by any person of the Confidential Information which may come to its attention and take all steps reasonably necessary to limit, stop or otherwise remedy such misappropriation, disclosure, or use caused or permitted by a [CONTRACTOR] employee.

6. **Duties Respecting Third Parties.** If [CONTRACTOR] will have access to the proprietary information of other companies in performing Task Order support services for the Government, [CONTRACTOR] shall enter into agreements with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. [CONTRACTOR] agrees to maintain copies of these third party agreements and furnish them to the Government upon request in accordance with 48 C.F.R. § 9.505-4(b).
7. **Notice Concerning Organizational Conflicts of Interest.** [CONTRACTOR] agrees that distribution, disclosure or dissemination of Confidential Information (whether authorized or unauthorized) within its corporate organization or affiliates, may lead to disqualification from participation in future Government procurements under the organizational conflict of interest rules of 48 C.F.R. § 9.5.
8. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties and supersedes any prior or contemporaneous oral or written representations with regard to protection of Confidential Information in performance of the subject Task Order. This Agreement may not be modified except in writing signed by both parties.
9. **Governing Law.** The laws of the United States shall govern this agreement.
10. **Severability.** If any provision of this Agreement is invalid or unenforceable under the applicable law, the remaining provisions shall remain in effect.

In accordance with Public Law No. 108-447, Consolidated Act, 2005, the following is applicable:

These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste,

fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.

11. Beneficiaries. If information owned by an individual or entity not a party to this agreement is disclosed or misappropriated by [CONTRACTOR] in breach of this agreement, such information owner is a third party beneficiary of this agreement. However, nothing herein shall create an independent right of action against the U.S. Government by any third party.

IN WITNESS WHEREOF, GSA and [CONTRACTOR] have caused the Agreement to be executed as of the day and year first written above.

UNITED STATES GENERAL SERVICES ADMINISTRATION

Name

Date

Contracting Officer

[CONTRACTOR]

Name*

Date

Title

*Person must have the authority to bind the company.

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

GSC-QF0B-15-32959

in support of:

Cyberspace Operations Support Services

in support of:

United States Cyber Command (USCYBERCOM)

FEDSIM Project Number AF00753

1.0 INTRODUCTION

This quality assurance surveillance plan (QASP) is pursuant to the requirements listed in the performance work statement (PWS) entitled Cyberspace Operations. This plan sets forth the procedures and guidelines General Services Administration (GSA) Federal System Integration and Management Center (FEDSIM) and United States Cyber Command (USCYBERCOM) will use in ensuring the required performance standards or services levels are achieved by the contractor.

1.1 PURPOSE

The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the contractor is meeting the performance standards/quality levels identified in the PWS and the contractor's quality control plan (QCP), and to ensure that the government pays only for the level of services received.

This QASP defines the roles and responsibilities of all members of the integrated project team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the contractor's performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results.

1.2 PERFORMANCE MANAGEMENT APPROACH

The PWS structures the acquisition around "what" service or quality level is required, as opposed to "how" the contractor should perform the work (i.e., results, not compliance). This QASP will define the performance management approach taken by GSA FEDSIM and USCYBERCOM to monitor and manage the contractor's performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyze information generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the contractor.

Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A "results" focus provides the contractor flexibility to continuously improve and innovate over the course of the contract as long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

1.3 PERFORMANCE MANAGEMENT STRATEGY

The contractor is responsible for the quality of all work performed. The contractor measures that quality through the contractor's own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this contract regardless of whether the work is performed by contractor employees or by subcontractors. The contractor's Quality Control Plan (QCP) will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The contractor will develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. This QASP enables the government to take advantage of the contractor's QC program.

The government representative(s) will monitor performance and review performance reports furnished by the contractor to determine how the contractor is performing against communicated performance objectives. The contractor will be responsible for making required changes in processes and practices to ensure performance is managed effectively.

2.0 ROLES AND RESPONSIBILITIES

2.1 Contracting Officer

The contracting officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by the contracting officer's representative (COR) and the contractor. The CO will designate one full-time COR as the government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, and must be identified and designated by the CO.

2.2 Contracting Officer Representative

The contracting officer's representative (COR) is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for technical administration of the project and ensures proper government surveillance of the contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COR will have the responsibility for completing Quality Assurance (QA) monitoring forms used to document the inspection and evaluation of the contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

3.0 IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS

The required performance standards and/or quality levels are included in the PWS and in Attachment 1, “Performance Requirements Summary.” If the contractor meets the required service or performance level, it will be paid the monthly amount agreed on in the contract.

4.0 METHODOLOGIES TO MONITOR PERFORMANCE

4.1 Surveillance Techniques

In an effort to minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate contractor performance when appropriate. The primary methods of surveillance are:

- Random monitoring, which shall be performed by the COR designated inspector.
- 100% Inspection – Each month, the COR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.
- Periodic Inspection – COR typically performs the periodic inspection on a monthly basis.

4.2 Customer Feedback

The contractor is expected to establish and maintain professional communication between its employees and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems but the customer always has the option to communicate complaints to the COR, as opposed to the contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COR. The COR will accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identified in Attachment 3.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.3 Acceptable Quality Levels

The acceptable quality levels (AQLs) included in Attachment 1, Performance Requirements Summary Table, for contractor performance are structured to allow the contractor to manage how the work is performed while providing negative incentives for performance shortfalls. Levels of performance are keyed to the relative importance of the task to the overall mission performance at USCYBERCOM.

5.0 QUALITY ASSURANCE DOCUMENTATION

5.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in the PWS and assessed using the performance monitoring techniques shown in Attachment 1.

5.2 Monitoring Forms

The government's QA surveillance, accomplished by the COR, will be reported using the monitoring forms in Attachments 2 and 3. The forms, when completed, will document the government's assessment of the contractor's performance under the contract to ensure that the required performance standards are being achieved.

The COR will retain a copy of all completed QA surveillance forms.

6.0 ANALYSIS OF QUALITY ASSURANCE MONITORING RESULTS

6.1 Determining Performance

Government shall use the monitoring methods cited to determine whether the performance standards have been met. If the contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

6.2 Reporting

At the end of each month, the COR will prepare a written report for the CO summarizing the overall results of the quality assurance surveillance of the contractor's performance. This written report, which includes the contractor's submitted monthly report and the completed quality assurance monitoring forms (Attachment 2), will become part of the QA documentation. It will enable the government to demonstrate whether the contractor is meeting the performance standards, including cost/technical/scheduling objectives.

6.3 Reviews and Resolution

The COR may require the contractor's project manager, or a designated alternate, to meet with the CO, COR and other government IPT personnel as deemed necessary to discuss performance evaluation. The CO or COR will define a frequency of in-depth reviews with the contractor, including appropriate self-assessments by the contractor; however, if the need arises, the contractor will meet with the CO or COR as often as required or per the contractor's request. The agenda of the reviews may include:

- Monthly performance assessment data and trend analysis
- Issues and concerns of both parties

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

- Projected outlook for upcoming months and progress against expected trends, including a corrective action plan analysis
- Recommendations for improved efficiency and/or effectiveness
- Issues arising from the performance monitoring processes.

The COR must coordinate and communicate with the contractor to resolve issues and concerns regarding marginal or unacceptable performance.

The COR and contractor should jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels should be clearly documented. Changes to service levels, procedures, and metrics will be incorporated as a contract modification.

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

ATTACHMENT 1: PERFORMANCE REQUIREMENTS SUMMARY

Required Services (Tasks)	Performance Standards	Acceptable Quality Levels	Methods of Surveillance
Submit a Program Management report of scheduled, completed, and outstanding tasks monthly.	100% of reports accurately depict current status	95% of the time	File reviews, periodic inspections, and random, observations, customer complaints
Administer QC program including subcontractor management in accordance with QCP	Contractor is in compliance with QCP 97% of the time	95% of the time	File reviews, periodic inspections, and random, observations, customer complaints
Trip Report(s)	Within 3 workdays following completion of each trip	95% of the time	100% Inspection Document Review
In-Progress Review (IPR)	Quarterly	95% of the time	100% Inspection Document Review
Deliverables and Reports. The Contractor submits all deliverables outlined in the TO.	95% accuracy of the deliverables/reports and are corrected within five (5) business days. The remaining 5% of the documented discrepancies cause no slip in schedule.	95% resolved in 5 days. No slip in schedule.	100% Inspection Document Review

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Invoices. CPFF Labor Submission	CPFF Labor invoices are accurate (i.e., amounts, backup documentation) and submitted no later than two months after the work is performed.	90% of the time	Monthly surveillance
Invoices. Cost Reimbursement CLINs (i.e., Travel, Tools & ODCs) Invoice Submission	Invoice Submission Cost incurred for Travel, Tools & ODCs are accurate (i.e., amounts, backup documentation) and invoiced no later than two months after a trip is taken or a purchased has occurred.	90% of the time	Monthly surveillance
Quality of Service. The Contractor conforms to overall contract requirements.	98% of documented discrepancies are resolved within five (5) business days and cause no slip in schedule. The remaining 2% of documented discrepancies cause no slip in schedule.	98% resolved in 5 days. No slip in schedule.	Monthly surveillance

ATTACHMENT 2

SAMPLE QUALITY ASSURANCE MONITORING FORM

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

ATTACHMENT 3

QUALITY ASSURANCE MONITORING FORM –
CUSTOMER COMPLAINT INVESTIGATION

SERVICE or STANDARD:

SURVEY PERIOD: _____

DATE/TIME COMPLAINT RECEIVED: _____ AM / PM

SOURCE OF COMPLAINT: _____ (NAME)

_____ (ORGANIZATION)

_____ (PHONE NUMBER)

_____ (EMAIL ADDRESS)

NATURE OF COMPLAINT:

RESULTS OF COMPLAINT INVESTIGATION:

DATE/TIME SERVICE PROVIDER INFORMED OF COMPLAINT: _____ AM / PM

CORRECTIVE ACTION TAKEN BY SERVICE PROVIDER:

RECEIVED AND VALIDATED BY:

PREPARED BY: _____

DATE: _____

**Attachment K –
ACRONYM LIST**

Acronym	Definition
ANSI	American National Standards Institute
C4	Command and Control
CAF	Contract Access Fee
CCIR	Commander's Critical Information Requirements
CCMD	Combatant Command
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CLIN	Contract Line Item Number
CMF	Cyber Mission Force
CMT	Combat Mission Teams
CST	Combat Support Teams
CO	Contracting Officer
COA	Courses of Action
CONOPS	Concepts of Operations
COR	Contracting Officer's Representative
CPAF	Cost-Plus-Award-Fee
CPFF	Cost-Plus-Fixed-Fee
CPARS	Contractor Performance Assessment Reporting System
CPT	Cyber Protection Teams
CTP	Consent to Purchase
DD	Department of Defense
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODIN	Department of Defense Information Networks
DSSR	Department of State Standardized Regulations
EEFI	Essential Elements of Friendly Information
EIT	Electronic and Information Technology
EST	Eastern Standard Time
ETC	Estimate to Completion
EV	Earned Value
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FEDSIM	Federal Systems Integration Management Center
FFP	Firm-Fixed-Price
FOIA	Freedom of Information Act
FSS	Federal Supply Schedule
FTE	Full Time Equivalent
FTR	Federal Travel Regulation
GFI	Government-Furnished Information
GFP	Government-Furnished Property

Acronym	Definition
GSA	General Services Administration
GSAM	General Services Administration Acquisition Manual
GWAC	Government Wide Agency Contract
IA	Interagency Agreement
IDIQ	Indefinite Delivery/Indefinite Quantity
IC	Intelligence Community
IT	Information Technology
JELC	Joint Event Lifecycle
JFHQs	Joint Forces Headquarters
JMET	Joint Mission Essential Tasks
JOPP	Joint Operation Planning Process
JTR	Joint Travel Regulation
LH	Labor Hour
MESL	Master Scenario Events List
MS	Microsoft
MSR	Monthly Status Report
MTT	Mobile Training Teams
NDAA	National Defense Authorization Act
NLT	No Later Than
NMT	National Mission Teams
NST	National Support Teams
NSP	Not Separately Priced
NTE	Not-to-Exceed
OCI	Organizational Conflict of Interest
OCO	Ordering Contracting Officer
ODC	Other Direct Costs
PIR	Priority Intelligence Requirements
POC	Point of Contact
PPIRS	Past Performance Information Retrieval System
PM	Project Manager
PMP	Project Management Plan
PNR	Problem Notification Report
PS	Project Start
PTE	Persistent Training Environment
PV	Planned Value
Q&A	Question and Answer
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan
RFP	Request for Proposal
RIP	Request to Initiate Purchase
SAP	Special Access Program
SAR	Situational Awareness Report
SEP	System Engineering Plans
SF	Standard Form

Acronym	Definition
SLA	Service Level Agreements
SOO	Statement of Objectives
SOP	Standard Operating Procedures
SOW	Statement of Work
SPI	Schedule Performance Index
T&M	Time and Materials
TBD	To Be Determined
TO	Task Order
TEB	Technical Evaluation Board
TOA	Task Order Award
TOR	Task Order Request
TOS	Tracking and Ordering System
TPOC	Technical Point of Contact
TTP	Tactics, Techniques, and Procedures
TTX	Table Top Exercises
U.S.	United States
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
WBS	Work Breakdown Structure



eSRS Contractor User Guide

Last Updated January 23, 2015

Disclosure: This Instruction manual has been prepared solely for the benefit of eSRS users. By accepting delivery of this Instruction Manual, the recipient hereby agrees that the information contained in this Instruction Manual, in whole or part, is confidential and proprietary and that it will not reproduce or redistribute such Instruction Manual, discuss the information contained herein or make reproductions without the prior written approval of the IAE, and will hold all information in confidence.

Revision Notes:

Revision	Date	Description
1.1	01/23/2015	Updates to Reporting Instructions manual refresh, corrections, and added references to additional resources for users.



Table of Contents

SECTION 1 ESRS BASICS	5
1.1 SYSTEM BACKGROUND.....	5
1.2 ABOUT THIS USER GUIDE.....	5
1.3 GETTING HELP WITH ESRS	6
1.3.1 THE HELP DESK.....	6
1.3.2 RESOURCES PAGE	8
1.3.3 ADDITIONAL RESOURCES	9
1.4 LOG-IN TO ESRS.....	9
1.4.1 SYSTEM TIED WITH FSRS.....	9
1.4.2 EXISTING USERS	9
1.4.3 NEW USERS.....	10
1.5 TERMS OF USE AGREEMENT	11
SECTION 2 NAVIGATION OVERVIEW	12
2.1 HOME.....	12
2.2 MAIN NAVIGATION OVERVIEW	13
SECTION 3 CONTRACT WORKLIST	16
3.1 VIEW EXISTING	16
3.2 ADD TO WORKLIST.....	17
SECTION 4 INDIVIDUAL SUBCONTRACT REPORTS	18
4.1 VIEW EXISTING	18
4.2 FILE A NEW INDIVIDUAL SUMMARY SUBCONTRACT REPORT	19
SECTION 5 SUMMARY SUBCONTRACT REPORTS.....	21
5.1 VIEW EXISTING	21



5.2 FILE A NEW SUMMARY SUBCONTRACT REPORT	22
<u>SECTION 6 FILING REPORTS AS A SUBCONTRACTOR</u>	<u>23</u>
<u>SECTION 7 YEAR-END SUPPLEMENTARY REPORT FOR SDBS</u>	<u>24</u>
7.1 VIEW EXISTING	24
7.2 FILE A NEW YEAR-END SUPPLEMENTARY REPORT	25
<u>SECTION 8 SDB PARTICIPATION REPORT (FORM 312)</u>	<u>26</u>
8.1 VIEW EXISTING	26
8.2 FILE A NEW SDB PARTICIPATION REPORT	27
<u>SECTION 9 BATCH UPLOAD REPORTS</u>	<u>28</u>
<u>SECTION 10 CUSTOM REPORTS.....</u>	<u>29</u>
10.1 BUILD NEW REPORTS.....	29
10.2 VIEW GENERATED REPORT	31
10.3 VIEW EXISTING REPORTS	32



Section 1 eSRS Basics

1.1 System Background

As part of the President's Management Agenda for Electronic Government, the Small Business Administration (SBA), the Integrated Acquisition Environment (IAE), and a number of Agency partners collaborated to develop the next generation of tools to collect subcontracting accomplishments. This government-wide tool is known as the eSRS. This Internet-based tool will streamline the process of reporting on subcontracting plans and provide agencies with access to analytical data on subcontracting performance. Specifically, the eSRS eliminates the need for paper submissions and processing of the SF 294's, Individual Subcontracting Reports, and SF 295's, Summary Subcontracting Reports, and replaces the paper with an easy-to-use electronic process to collect the data.

To learn more, please review the home page materials that discuss the system's background, reporting requirements, and the eSRS legislation, regulations and OMB Guidance.

1.2 About this User Guide

This user guide is intended for Contractor users of the eSRS.gov system who are required to complete their subcontract reporting for federally awarded contracts. The guide will help these users utilize the system to create and manage their contract reporting and review their sub-contractor reports. Both Prime and Sub contractor reporting is completed in the eSRS.gov system.

1.3 Getting Help with eSRS

1.3.1 The Help Desk

- I. Users can access the Federal Service Desk (FSD) directly from within the system. FSD is the help desk organization that provides help desk support for eSRS.gov.
- II. A link to the FSD is presented on the home page in the right-hand side bar. This link can also be found when logged into the system at the bottom of each page.

Navigation to Access FSD on eSRS.gov

Documents

User Guides

» [FSRS Awardee Guide](#)

Training Materials

» [FSRS Awardee User Demonstration](#)

News

Question of the Month:

Who is required to file a FFATA report in FSRS? [View the answer](#)

New! As of October 29, 2010, FSRS.gov now supports both contracts and grants sub-award reporting. Prime awardees, [click here](#) to register or log-in.

Viewer Software:

Some documents linked from this page are in PDF, Flash, or PowerPoint format. To view these files, you may need to download:

» [Adobe Acrobat Reader](#)
» [Adobe Flash Player](#)
» [Microsoft PowerPoint Viewer 2007](#)

For questions about FSRS, contact:

» Your contracting officer for questions about FSRS applicability to your contracts.

» [For Help: Federal Service Desk](#)



- III. Clicking on the FSD link opens a transition page introducing the Federal Service Desk (FSD) where users can secure assistance.

FSD Transition Page

The screenshot shows the Federal Service Desk transition page. At the top, there is a header bar with the eSRS logo and text: "eSRS Integrated Acquisition Environment Electronic Subcontracting Reporting System". Below this, a blue banner features the "Federal Service Desk" logo and the text "Start here for help on US Government contracts." Below the banner, a message states: "You will be re-directed to the Federal Service Desk in 30 seconds. Click the logo above if you would like to be redirected immediately." The main content area begins with "INTRODUCING..." followed by the heading "The Federal Service Desk". Underneath, it says "eSRS Users:" and then provides a paragraph of information about the FSD. This is followed by a bulleted list of services available at the FSD. At the bottom, there is a paragraph about the transition of other systems to FSD and a link to the "Privacy Policy".

Federal Service Desk
Start here for help on US Government contracts.

You will be re-directed to the Federal Service Desk in 30 seconds. Click the logo above if you would like to be redirected immediately.

INTRODUCING...

The Federal Service Desk

eSRS Users:

We are pleased to introduce you to a new source of help for your questions concerning the Electronic Subcontracting Reporting System (eSRS). Although FSD will be handling technical calls only, you will be able to submit a non-technical question via the "Submit New Request" or speak to a representative to receive the email address of the eSRS Agency Coordinator and Point of Contact for the Agency you are reporting to or the Small Business Administration's (SBA) Procurement Analyst assigned to answer Subcontracting questions.

The Federal Service Desk (FSD) launched in June 2009 as a project of the GSA's Integrated Acquisition Environment (IAE). At the Federal Service Desk (fsd.gov) you can now:

- Find information you need by searching several ways in the Answer Center
- Submit a request online for Non-Technical (Policy) and Technical service
- Check on your help desk ticket online
- Give us feedback on Frequently Asked Questions
- Chat live with a Customer Service Representative
- Phone us toll free at 1-866-606-8220
- Phone us internationally at 334-206-7828

Over the next year or so, additional systems will gradually transition to FSD for their help desk support. We hope you take advantage of the full range of services offered at www.fsd.gov.

[Privacy Policy](#)

- IV. Users are automatically re-directed to the FSD 30 seconds after navigating to the transition page.



1.3.2 Resources Page

- I. When logged into the system, in the main navigation bar at the bottom of any system page, users will see a link to access a resources page. This page presents resources for the user related to the utilization of the eSRS system.

Resources Page

Resources

Quick Reference Guides

- [Quick Reference for Federal Government Contractors Filing SSR for Commercial Plan](#)
- [Quick Reference for Federal Government Contractors Filing SSR for Individual Plan](#)
- [Quick Reference for Federal Government Contractors Submitting SDB Participation Report](#)
- [Quick Reference for Federal Government Contractors Submitting SDB Year-End Report](#)
- [Quick Reference for Federal Government Prime Contractors Filing ISR](#)
- [Quick Reference for Federal Government Subcontractors Filing ISR](#)
- [Quick Reference Recommendation for Federal Government Employees Generating Reports](#)

Webinars

For Contractor Users:	For Government Users:
<ul style="list-style-type: none">• Contractor Submitting an Individual Subcontract Report (ISR)• Contractor Submitting an Summary Subcontract Report (SSR - Individual)	<ul style="list-style-type: none">• Government Review of the Individual Subcontract Report (ISR)• Government Review of the Summary Subcontracting Report (SSR)

- II. On this page, users will find Quick Reference Guides and Webinars.



1.3.3 Additional Resources

At the bottom of every page, when logged into the system, additional contractor references are provided. This includes specific individual instructions for each report type. This user guide provides a general reference to using the system and the quick reference guides provide specific guidance on completing reports.

Additional Quick Reference Links – Bottom of page

For Help: [Federal Service Desk](#) [Turn Accessibility Mode On](#) [Contractor User Guide](#) [Registration Instructions for Contractors](#) [SSR for Individual Plan](#) [Prime Filing ISR](#) [SSR for Commercial Plan](#) [Subcontractor Filing ISR](#) [SDB Participation Report](#) [SDB Year End Report](#) [Generating Reports](#) [Contractor Submitting an Individual Subcontract Report \(ISR\)](#) [Contractor Submitting an Summary Subcontract Report \(SSR - Individual\)](#) Version 3.4

1.4 Log-In to eSRS

1.4.1 System Tied with FSRS

Users registered in the Federal Funding Accountability and Transparency Act Subaward Reporting System (www.fsr.gov) are able to access the eSRS system with the same log-in credentials as used for FSRS. If you register for a new account in the eSRS system, you will be able to login to the FSRS system with the same credentials. In addition, authenticated (logged-in) users are able to toggle between the eSRS.gov and FSRS.gov applications seamlessly by clicking on the link in the upper right hand corner of any page, "Log-in to eSRS" or "Log-in to FSRS," depending on the system in which you are currently working.

FSRS Log-In Link when Logged into eSRS.gov



1.4.2 Existing Users

- I. Point your browser to <https://www.esrs.gov>
- II. Click on Contractors in the Log-In or Register Now box
- III. Login to eSRS by typing your e-mail address and password.
- IV. Click Go to enter the system

eSRS Log-In or Register Now



Contractor User Sign-In

login

returning contractors: login

Email:

Password:

[Login](#) [Forgot Password](#)

new contractors: register

Register for a new account

[Register](#)

[Registration Instructions for Contractors](#)

[Contractor User Guide](#)

[Not a contractor user? Click here.](#)

1.4.3 New Users

- I. Users point their browser to <https://www.esrs.gov>. **NOTE: Users do not need to re-register if they have an existing FSRS Awardee user account (www.fsrs.gov).** The email address and password used for FSRS will allow the user to log-in to eSRS.gov.
- II. The agency user clicks on the “Contractors” link within the “Log-In or Register Now” box.
- III. To register, the user clicks the “Register” tab under the new contractors: register section
- IV. The user completes the multi-step process that displays. **Note: Throughout the system a red asterisk (*) designates that the field is required.**
- V. Step 1: The user enters their organization’s DUNS Identification Number and clicks the “Next” button.



Contractor Registration Screen Step 1

Registration Step 1 of 2

Please enter your DUNS Identification Number.

(Previously, this field was called the "Contractor Identification Number.") Please do not include any dashes when entering your DUNS number. Upon entering the DUNS, FSRS will pull the appropriate company information from the System for Award Management (SAM) database and auto-populate most of the fields on the next screen. You will still need to fill in the required Contact Information fields. (If the auto-populated information is incorrect, you'll need to contact SAM rather than FSRS.)

Note: If you have an account in eSRS (<https://www.esrs.gov>) you do not have to re-register here. You may use the same username/password for both systems.

Note: Only the prime contractor's representative can register under their DUNS # to file a report. By registering under this DUNS # you certify that you are a representative of the prime contractor's company and have the authority to file this report.

Note

Please be aware that all information collected on the FSRS website (www.fsrs.gov), including registration information and report data, will be visible to the public on a public website (www.usaspending.gov).

DUNS #

- VI. On Step 2, some form data may already be populated on the form from SAM.gov (System for Award Management). This is based on the DUNS entered in Step 1.
- VII. Users must complete all required fields and click the "Submit" button.
- VIII. After submitting this form, a confirmation email is sent to the email address provided during the registration process. The email presents instructions on how to finalize the registration process. **Note: An account is only activated after the user follows the instructions presented in the email.**
- IX. After a user has confirmed their registration, as outlined in the email, the user can return to the Login-In page (see Existing Users, page 15). They can then enter their email address and password, and click the "Login" button, to log-in to eSRS.

1.5 Terms of Use Agreement

- I. All users are required to agree to the Terms of Use for eSRS.
- II. Use the side scroll bar resource to review the terms and conditions in their entirety.
- III. A user can click "OK" to move forward or "Log-Off" to exit the system.



Terms of Use Agreement Screen

The screenshot shows the "eSRS Terms and Conditions" screen. At the top, there is a header bar with the eSRS logo and the text "Integrated Acquisition Environment Electronic Subcontracting Reporting System". Below the header, the title "eSRS Terms and Conditions" is displayed. A paragraph of text reads: "LOG OFF IMMEDIATELY if you do not consent to the conditions stated in the following notice. Otherwise click OK to accept the terms and proceed." Below this, there is a scrollable area containing two sections: "I. Usage Agreement" and "II. Privacy Act Routine Uses (5 USC § 522a as amended)". The "Usage Agreement" section contains a detailed paragraph about the system's ownership by the United States Government and the terms of use. The "Privacy Act Routine Uses" section is partially visible. At the bottom of the scrollable area, there are two buttons: "OK" and "Log-Off". Below the buttons, there is a link "For Help: Federal Service Desk" and the text "Version 3.4".

Section 2 Navigation Overview

2.1 Home

- I. Login to eSRS.
- II. You will be directed to your eSRS Home page.
- III. On the left hand side of the screen a navigation menu is shown. These are Quicklinks to completing the different report types available in eSRS.



- IV. Alerts will display all items in the system that requires your immediate attention such as Rejected reports.
- V. Finally, when you are done using the system, please click on the “Logout” link on the top of every page.

Contractor Users Homepage

add contract to worklist	alerts • No current alerts
file ISR <small>(FORMERLY SF-294)</small>	announcements • NASA Class Deviation on SSRs On November 21, 2013, NASA issued a Class Deviation for Summary Subcontract Report (SSR)-Submission under Individual Subcontracting Plans, which eliminates the requirement to submit a mid-year SSR for individual plans. The Deviation applies to solicitations issued on or after November 21, 2013. For contractors holding NASA contracts that were awarded before this date and that contain subcontracting plans, a mid-year SSR is still required unless all such contracts are modified to include the Deviation. Contractors may request Contracting Officers to modify existing contracts to include the Deviation. For additional information, refer to NASA Procurement Information Circular (PIC) 13-06B located here: http://www.hq.nasa.gov/office/procurement/regs/pic13-06B.html . Questions may be directed to Richard Mann at 202-358-2438.
file SSR <small>(FORMERLY SF-295)</small>	
file year-end supplementary report <small>(FOR SDBs)</small>	
file SDB participation report <small>(FORMERLY OF-312)</small>	

2.2 Main Navigation Overview

The Contractor user’s main navigation runs horizontally along the top of the page.

myESRS: myESRS will return you to the default home page upon login.

Profile: The profile page allows you to edit your account and contact information. Please turn to “Section 3, Profile” of this manual for more information.

Contract Worklist: The Contract worklist allows you to view all contracts that have been linked to your account. Please turn to “Section 4, Contract Worklist” of this manual for more information.



File / Review Reports:

Individual Subcontract Reports: The Individual Subcontract Reports area allows you to add and review ISR's. Please turn to "Section 5, Individual Subcontract Reports" of this manual for more information.

Summary Subcontract Reports: The Summary Subcontract Reports area allows you to add and review SSR's. Please turn to "Section 6, Summary Subcontract Reports" of this manual for more information.

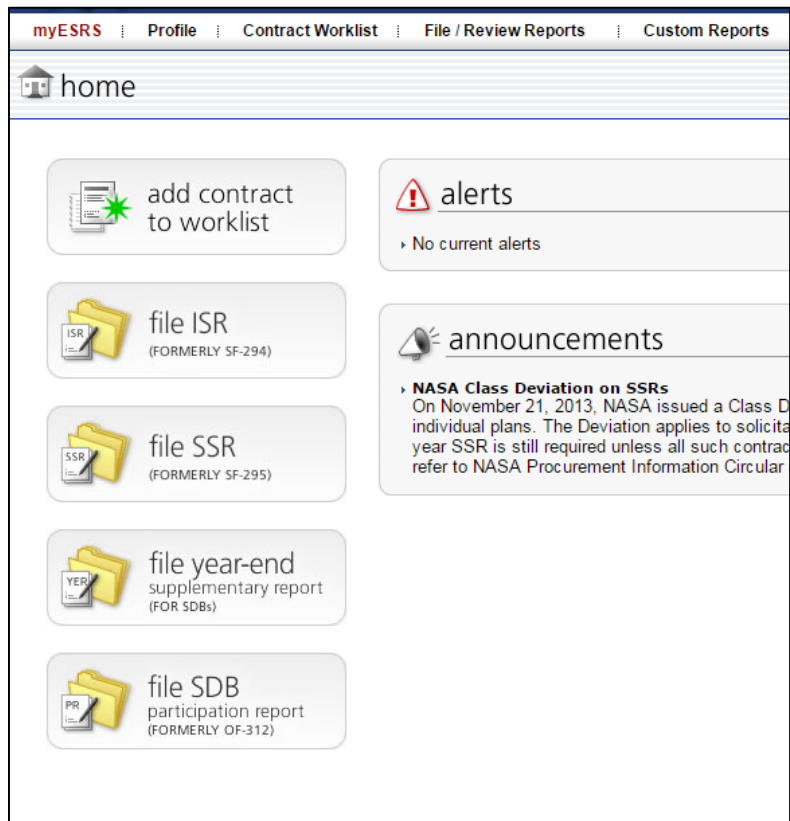
Year-End Supplementary Report for SDBs: This section allows you to file and/or review Year-End Supplementary Report for SDBs. Please go to "Section 8, Year-End Supplementary Report for SDBs" of this manual for more information.

SDB Participation Report (Form 312): This section allows you to file and/or review the optional SDB Participation Report (Form 312). Please go to "Section 9, Year-End Supplementary Report for SDBs" of this manual for more information.

Batch Upload Reports: The batch upload section allows you to download a Microsoft® Excel™ template that can then be exported to a CSV (comma separated value) or tab delimited file and then imported into eSRS. This feature allows you to file multiple reports at once. Please see "Section 10, Batch Uploads" of this manual for more information.

Custom Reports: Allows the user to run ad hoc and pre-defined reports provided by the system

Contractor Navigation



Section 3 Contract Worklist

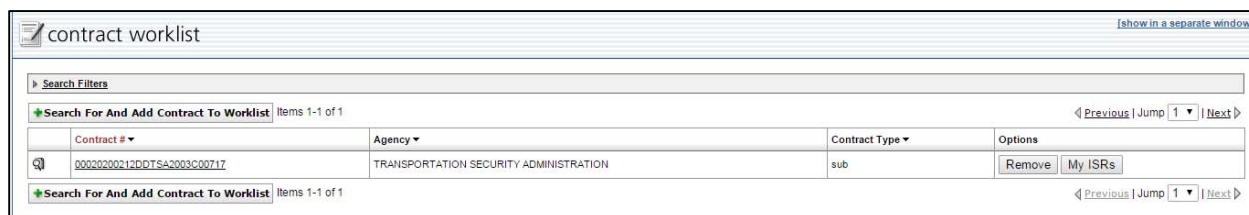
3.1 View Existing

- I. Click on “Contract Worklist” on the navigation bar.
- II. A screen similar to the “Contract List Screenshot” below will appear.
- III. You may sort the list of contracts. This is accomplished by clicking on the text next to any down arrow in the column headings. You may sort the list in ascending order if you click on the same heading again. Note how the color of the text changes. The current active column is designated by a **Maroon** color.
- IV. To view the details of an existing contract, click on the View Icon beside the contract, or click on the Contract Number.
- V. You are now able to review more information regarding the contract. If you wish to edit the information at this time, click on the button next to the appropriate Contract Number from within the “My Contractor ISRs” tab .
- VI. You can also enter reports or view-lower tier reports. Click on the tabs beside the “Contract Details” tab to toggle between the views.

(Note: for more information regarding adding reports, please see the corresponding section of this manual)

- VII. After entering “Edit Mode” click the “Save” button to save your changes.

Contract Worklist



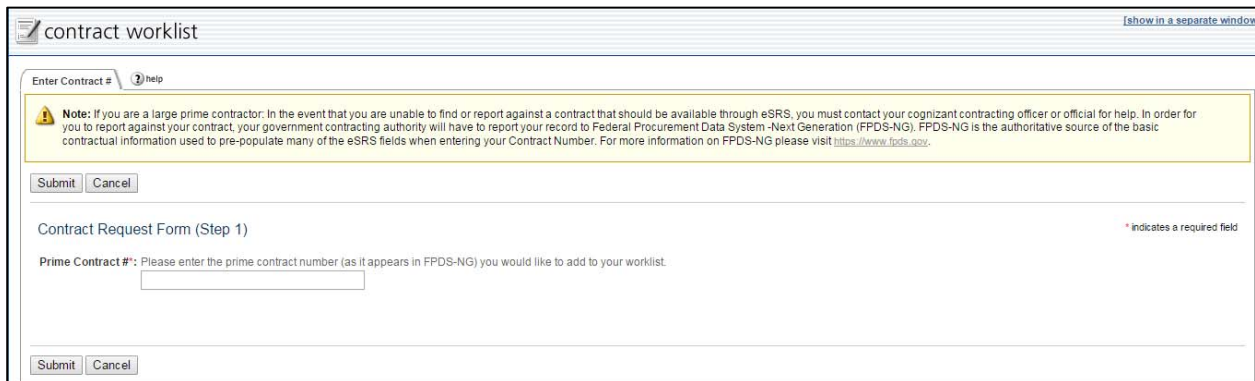
Contract #	Agency	Contract Type	Options
00020200212DDTSA2003C00717	TRANSPORTATION SECURITY ADMINISTRATION	sub	Remove My ISRs

3.2 Add to Worklist

There are two different methods to add a new contract to your account. The first method allows you to easily add a new contract from the “myESRS” homepage. Simply click on the “Add Contract to Worklist” button or follow the method below.

- I. Click on “Contract Worklist” on the navigation bar.
- II. To add a new contract to your worklist, click on the Add New Contract to Worklist button.
- III. Enter the Prime Contract # (as it appears in FPDS-NG). **Note: If a Contract # changes in FPDS-NG, you will only be able to search on the current #.**
- IV. Click Submit
- V. Select whether your organization is a “Prime” or “Subcontractor”.
- VI. You will now be directed to the “contract details” page for the contract you just added. To return to the Contract Worklist, click on the “Back To List” link within the system (**Note: Do not click your browser’s back button**).

Add to Worklist



contract worklist [show in a separate window](#)

Enter Contract # [help](#)

Note: If you are a large prime contractor: In the event that you are unable to find or report against a contract that should be available through eSRS, you must contact your cognizant contracting officer or official for help. In order for you to report against your contract, your government contracting authority will have to report your record to Federal Procurement Data System -Next Generation (FPDS-NG). FPDS-NG is the authoritative source of the basic contractual information used to pre-populate many of the eSRS fields when entering your Contract Number. For more information on FPDS-NG please visit <https://www.fpds.gov>.

Contract Request Form (Step 1) * indicates a required field

Prime Contract #*: Please enter the prime contract number (as it appears in FPDS-NG) you would like to add to your worklist.

Section 4 Individual Subcontract Reports

4.1 View Existing

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on Individual Subcontract Reports on the drop down.
- III. You will be directed to a screen similar to the “Individual Subcontract Reports Screenshot” below.
- IV. The status for each report is displayed in the status column.
Notice on the bottom of the page, a legend appears:

DRT = Draft	PEN = Pending	REV = Revised	ACC = Accepted	REJ = Rejected
--------------------	----------------------	----------------------	-----------------------	-----------------------

Draft: You began working on a report, however did not complete it and/or submit it for approval.

Pending: The report has been submitted and is awaiting acceptance from the appropriate government official.

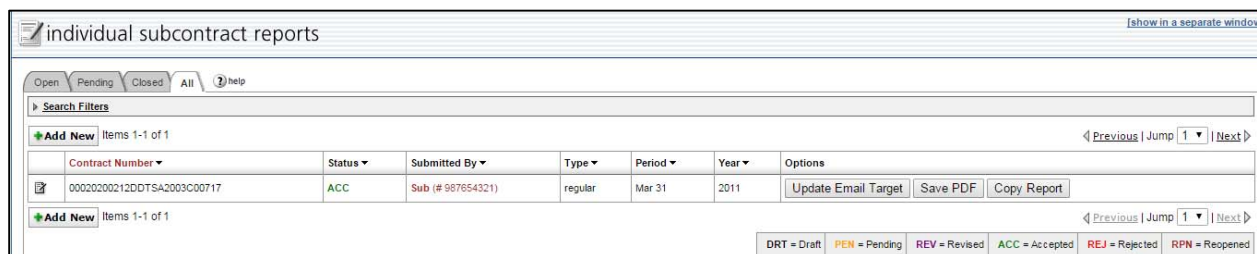
Revised: The report has been revised by a government official.

Accepted: A government official has accepted your report.

Rejected: A government official has rejected your report.

- V. To view the details of a submitted report, click on the Icon beside the report.
- VI. If the report has been rejected, you may click on the “Notes” tab to view the reason why the report has been rejected.
- VII. To return to the report list, click the “Cancel” button at any time.

Individual Subcontract Report Listing




individual subcontract reports [\[show in a separate window\]](#)

Open Pending Closed All [help](#)

[Search Filters](#)

[Add New](#) Items 1-1 of 1 [Previous](#) | [Jump](#) 1 | [Next](#)

Contract Number	Status	Submitted By	Type	Period	Year	Options
 00020200212DDTSA2003C00717	ACC	Sub (# 987654321)	regular	Mar 31	2011	Update Email Target Save PDF Copy Report

[Add New](#) Items 1-1 of 1 [Previous](#) | [Jump](#) 1 | [Next](#)

DRT = Draft PEN = Pending REV = Revised ACC = Accepted REJ = Rejected RPN = Reopened



4.2 File a New Individual Summary Subcontract Report

There are two different methods to file a new Individual Subcontract Report. The first method allows you to easily file a new Individual Subcontract Report from the myESRS Homepage. Click on the File ISR Quicklink button or follow the steps below.

- I. Click on "File / Review Reports" on the navigation bar.
- II. Click on Individual Subcontract Reports on the drop down.
- III. To file a new report, click on the Add New button.
- IV. You will be taken to the Instructions page similar to the screenshot below. Please take time to read the instructions.
- V. Click on the Continue button when ready.
- VI. Select a contract from the drop down box or manually enter the contract number. Click Continue. **Note: If the Contract # changed in FPDS-NG, you will only be able to search on the current #.**
- VII. Fill out the forms for each step and click "Save & Continue" or "Continue" to move to the next step of the process. (*Note: Click on the context sensitive help button beside the fields for more information*)
- VIII. On step 8, click the Submit button to send the report.
- IX. You may now return to view existing reports to view the status of the report you just entered.
- X. In order to completely submit the report, you must click "Submit" on step 8 (Designated on the left hand side of the screen) of the report submission process.

Note: On step 6 of the report submission process, you must fill out either the "Percentage of Total Subcontract Awards" OR "Percentage of Total Contract Value" field for Part 3. SMALL DISADVANTAGED BUSINESS (SDB) CONCERNS.

Individual Subcontract Report Instructions

individual subcontract reports [\[show in a separate w\]](#)

New Report

[+ BACK TO LIST](#)

1 Instructions

2 Enter Contract #

3 Contract Details

4 Subcontracting Report

5 Subcontracting Report Confd

6 Subcontract Awards

7 Review

8 Submit Report

Individual Subcontracting Reports

Please Note: the eSRS contains a number of new fields that did not exist on the paper forms. Although the eSRS will allow you to save a partially completed report, you will save time if you have the following information available when you enter your report data:

For Prime Contractors

- Your DUNS number as it appears on the contract
- Product and Service Description
- NAICS
- E-mail address of Federal Government Agency responsible for reviewing your report
- Current Contract Value
- Approved Small Business Individual Subcontracting Plan
- Be sure to keep a signed copy of the report on file

For Lower Tier Subcontractors

- The Prime contract number
- The Subcontract number
- The DUNS number of the contractor that awarded you the subcontract
- E-mail address of the contractor's employee who awarded you the contract and has the responsibility to review your subcontracting report.
- Product and Service Description
- NAICS
- Approved Small Business Individual Subcontracting Plan
- Be sure to keep a signed copy of the report on file

Copy Existing Report

Note: You may copy data from an existing report by selecting a report below.

Cancel Continue

Section 5 Summary Subcontract Reports

5.1 View Existing

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on Summary Subcontract Reports on the drop down.
- III. You will be directed to a screen similar to the “Summary Subcontract Reports Screenshot” below.
- IV. The status for each report is displayed in the status column.
Notice on the bottom of the page, a legend appears:

DRT = Draft **PEN** = Pending **REV** = Revised **ACC** = Accepted **REJ** = Rejected

Draft: You began working on a report, however did not complete it and/or submit it for approval.

Pending: The report has been submitted and is awaiting acceptance from the appropriate government official.

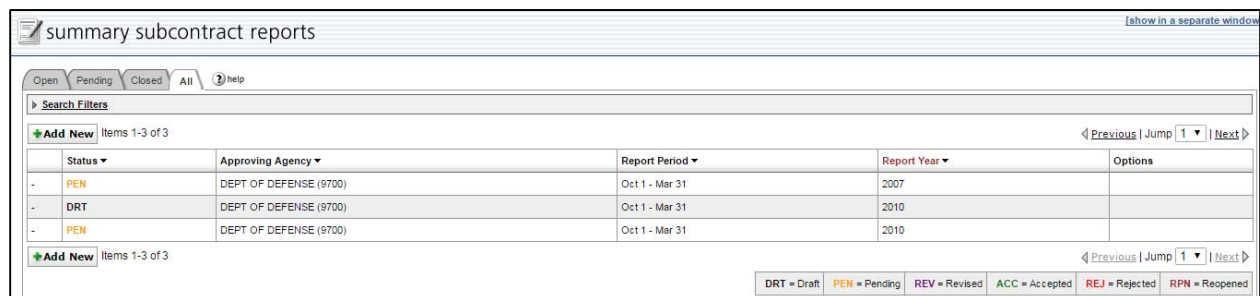
Revised: The report has been revised by a government official.

Accepted: A government official has accepted your report.

Rejected: A government official has rejected your report.

- V. To view the details of a submitted report, click on the View Icon beside the report.
- VI. If the report has been rejected, you may click on the “Rejection Notes” tab to view the reason why the report has been rejected.
- VII. To return to the report list, click the “Cancel” button at any time.

Summary Subcontract Reports Listing



summary subcontract reports [\[show in a separate window\]](#)

Open Pending Closed All ? help

Search Filters

[Add New](#) Items 1-3 of 3

Status ▼	Approving Agency ▼	Report Period ▼	Report Year ▼	Options
PEN	DEPT OF DEFENSE (9700)	Oct 1 - Mar 31	2007	
DRT	DEPT OF DEFENSE (9700)	Oct 1 - Mar 31	2010	
PEN	DEPT OF DEFENSE (9700)	Oct 1 - Mar 31	2010	

[Add New](#) Items 1-3 of 3

[Previous](#) | [Jump](#) 1 | [Next](#)

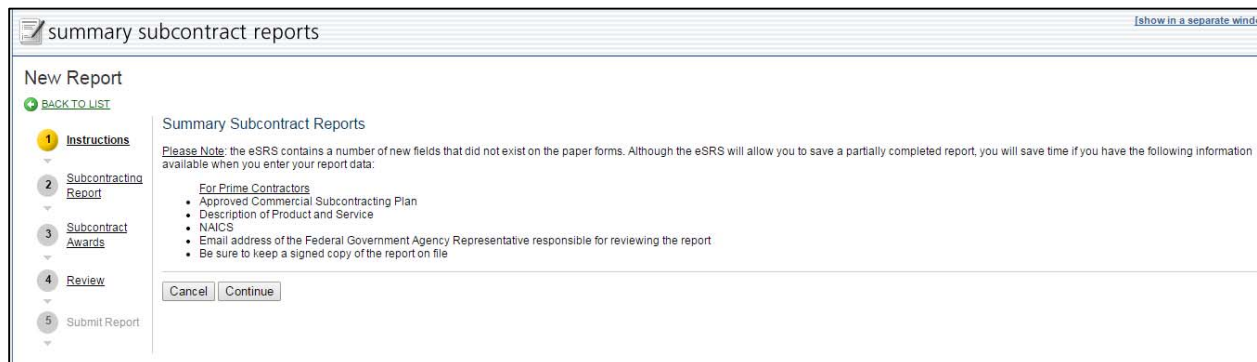
DRT = Draft PEN = Pending REV = Revised ACC = Accepted REJ = Rejected RPN = Reopened

5.2 File a New Summary Subcontract Report

There are two different methods to file a new Summary Subcontract Report. The first method allows you to easily file a new Summary Subcontract Report from the myESRS Homepage. Click on the File SSR Quicklink button or follow the steps below.

- I. Click on "File / Review Reports" on the navigation bar.
- II. Click on Summary Subcontract Reports on the drop down.
- III. To file a new report, click on the Add New button.
- IV. You will be taken to the instructions page similar to the screenshot below. Please take time to read the instructions.
- V. Click on the Continue button when ready.
- VI. Select the Agency that you wish to file a report to. *(If the report is a commercial plan report, you can select multiple agencies. Please make sure to select an approver.)*
- VII. Fill out the forms for each step and click "Save & Continue" or "Continue" to move to the next step of the process. *(Note, Click on the context sensitive help button beside the fields for more information)*
- VIII. On step 5, click the Submit button to send the report.
- IX. You may now return to view existing reports to view the status of the report you just entered.

Summary Subcontractor Report Instructions



summary subcontract reports [\[show in a separate window\]](#)

New Report

[BACK TO LIST](#)

1 Instructions

2 Subcontracting Report

3 Subcontract Awards

4 Review

5 Submit Report

Summary Subcontract Reports

Please Note: the eSRS contains a number of new fields that did not exist on the paper forms. Although the eSRS will allow you to save a partially completed report, you will save time if you have the following information available when you enter your report data:

For Prime Contractors

- Approved Commercial Subcontracting Plan
- Description of Product and Service
- NAICS
- Email address of the Federal Government Agency Representative responsible for reviewing the report
- Be sure to keep a signed copy of the report on file



Section 6 Filing Reports as a Subcontractor

Filing reports as a subcontractor allows the next higher tier contractor to see your filing. In order to correctly file a report as a “sub”, first select the type of report you wish to file. Although the eSRS will allow you to save a partially completed report, you will save time if you have the following information available when you enter your report data:

- A.) The Prime Contract Number
 - B.) The Sub Contract Number
 - C.) The DUNS number of the contractor that awarded you the subcontract
 - D.) E-mail address of the contractor's employee who awarded you the contract and has the responsibility to review your subcontracting report
 - E.) Product and Service Description
 - F.) NAICS
 - G.) Approved Small Business Individual Subcontracting Plan
 - H.) Be sure to keep a signed copy of the report on file
-
- I. Once you have begun filing your report (ISR or SSR) enter the contract number of the contract for which you wish to file.
 - II. Once you have entered the contract number, click Continue.
 - III. As a Subcontractor for this contract, you will now be forced to file as a “Sub”. Notice that the selection “Prime” is unavailable.
 - IV. Enter the DUNS# and e-mail address of the next available tier contractor.
 - V. Enter the Contract Amount.
 - VI. You may now progress through the report submission process by clicking the “Save and Continue” button after you have completed each step.
 - VII. In order to completely submit the report, you must click “Submit” on step 8 (Designated on the left hand side of the screen) of the report submission process.

Section 7 Year-End Supplementary Report for SDBs

7.1 View Existing

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on **Year-End Supplementary Report for SDBs** in the dropdown.
- III. You will be directed to a screen similar to the “Year End Section” below.
- IV. The status for each report is displayed in the status column.

Notice on the bottom of the page, a legend appears:

DRT = Draft	PEN = Pending	REV = Revised	ACC = Accepted	REJ = Rejected
--------------------	----------------------	----------------------	-----------------------	-----------------------


Draft: You began working on a report, however did not complete it and/or submit it for approval.

Pending: The report has been submitted and is awaiting acceptance from the appropriate government official.

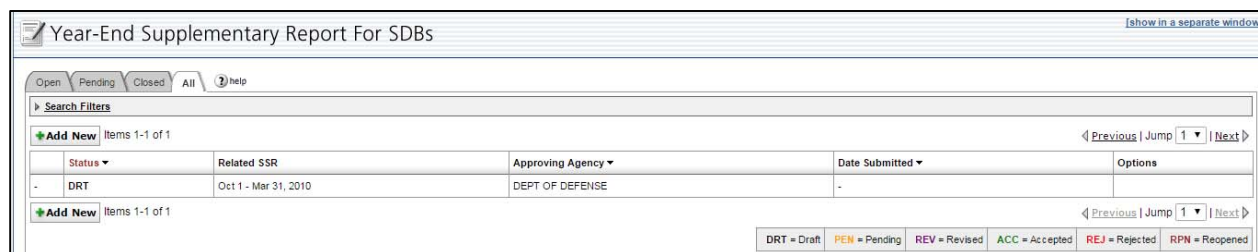
Revised: The report has been revised by a government official.

Accepted: A government official has accepted your report.

Rejected: A government official has rejected your report.

- V. To view the details of a submitted report, click on the  View Icon beside the report.
- VI. If the report has been rejected, you may click on the “Rejection Notes” tab to view the reason why the report has been rejected.
- VII. To return to the report list, click the “Cancel” button at any time.

Year-End SDB Listing



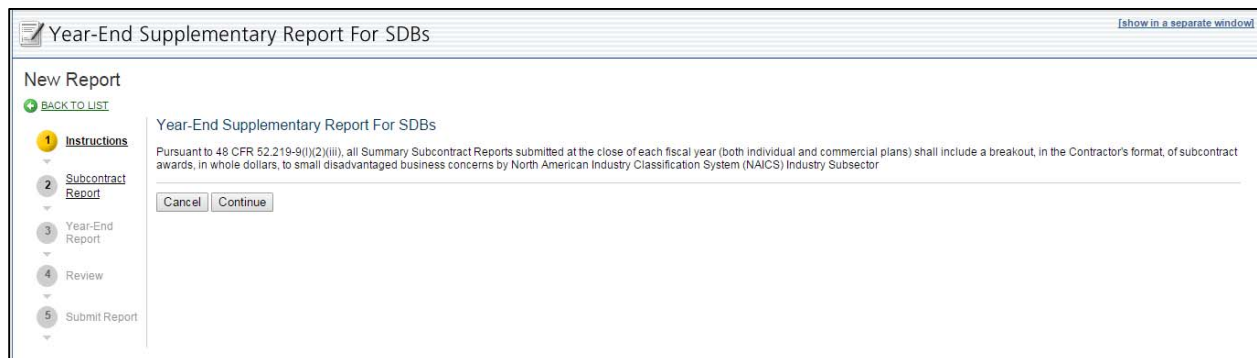
The screenshot shows the 'Year-End Supplementary Report For SDBs' interface. At the top, there are tabs for 'Open', 'Pending', 'Closed', and 'All', along with a 'help' icon. Below the tabs is a 'Search Filters' section. The main area displays a table with columns: 'Status', 'Related SSR', 'Approving Agency', 'Date Submitted', and 'Options'. The table contains one row with the status 'DRT' (Draft), 'Oct 1 - Mar 31, 2010' for the Related SSR, and 'DEPT OF DEFENSE' for the Approving Agency. The Date Submitted is blank. At the bottom right, there is a legend for the status codes: DRT = Draft, PEN = Pending, REV = Revised, ACC = Accepted, REJ = Rejected, and RPN = Reopened. Navigation links for 'Previous', 'Jump', and 'Next' are also present.

7.2 File a New Year-End Supplementary Report

There are two different methods to file a new Year-End Supplementary Report. The first method allows you to easily file a new Year-End Supplementary Report from the myESRS Homepage. Click on the File Year-End Quicklink button or follow the steps below.

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on “Year-End Supplementary Reports for SDBs” on the drop down.
- III. To file a new report, click on the Add New button.
- IV. You will be taken to the instructions page similar to the screenshot below. Please take time to read the instructions.
- V. Click on the Continue button when ready.
- VI. Select the Year-End Supplementary Report that the report should be associated with.
- VII. Fill out the forms for each step and click “Save & Continue” or “Continue” to move to the next step of the process. *(Note, Click on the context sensitive help button beside the fields for more information)*
- VIII. On step 5, click the Submit button to send the report.
- IX. You may now return to view existing reports to view the status of the report you just entered.

Year-End Supplementary Instructions



Year-End Supplementary Report For SDBs [\[show in a separate window\]](#)

New Report

[BACK TO LIST](#)

1 Instructions

2 Subcontract Report

3 Year-End Report

4 Review

5 Submit Report

Year-End Supplementary Report For SDBs

Pursuant to 48 CFR 52.219-9(i)(2)(iii), all Summary Subcontract Reports submitted at the close of each fiscal year (both individual and commercial plans) shall include a breakout, in the Contractor's format, of subcontract awards, in whole dollars, to small disadvantaged business concerns by North American Industry Classification System (NAICS) Industry Subsector

Section 8 SDB Participation Report (Form 312)

8.1 View Existing

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on **SDB Participation Report** in the dropdown.
- III. You will be directed to a screen similar to the “**SDB Participation Report**” below.
- IV. The status for each report is displayed in the status column.

Notice on the bottom of the page, a legend appears:

DRT = Draft	PEN = Pending	REV = Revised	ACC = Accepted	REJ = Rejected
--------------------	----------------------	----------------------	-----------------------	-----------------------

Draft: You began working on a report, however did not complete it and/or submit it for approval.

Pending: The report has been submitted and is awaiting acceptance from the appropriate government official.

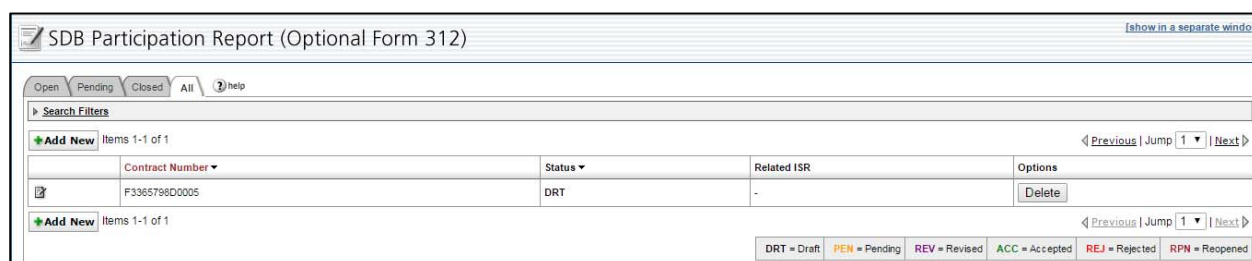
Revised: The report has been revised by a government official.

Accepted: A government official has accepted your report.

Rejected: A government official has rejected your report.

- V. To view the details of a submitted report, click on the View Icon beside the report.
- VI. If the report has been rejected, you may click on the “Rejection Notes” tab to view the reason why the report has been rejected.
- VII. To return to the report list, click the “Cancel” button at any time.

SDB Participation Listing




SDB Participation Report (Optional Form 312) [\[show in a separate window\]](#)

Open Pending Closed All ? help

Search Filters

[Add New](#) Items 1-1 of 1

Contract Number ▼	Status ▼	Related ISR	Options
 F3365798D0005	DRT	-	Delete

[Add New](#) Items 1-1 of 1

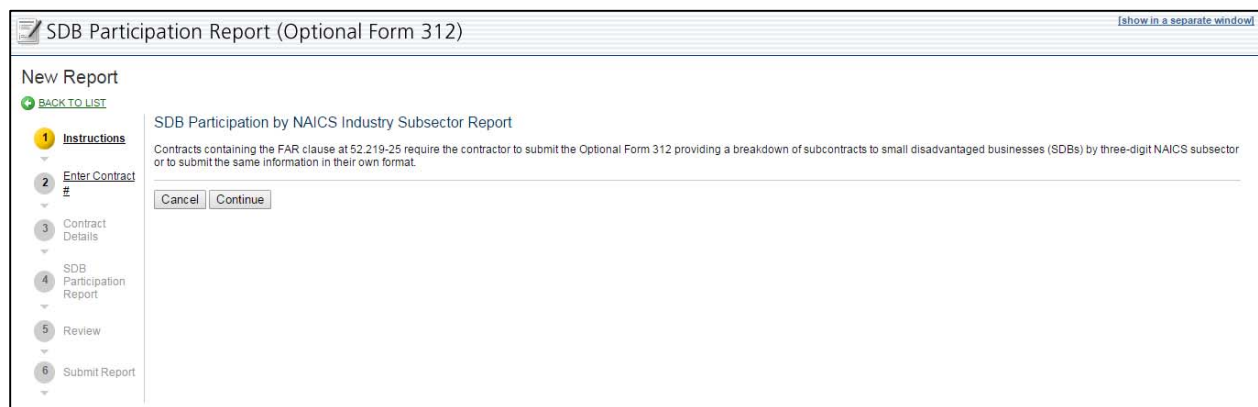
Legend: **DRT** = Draft **PEN** = Pending **REV** = Revised **ACC** = Accepted **REJ** = Rejected **RPN** = Reopened


8.2 File a New SDB Participation Report

There are two different methods to file a new SDB Participation Report. The first method allows you to easily file a new SDB Participation Report from the myESRS Homepage. Click on the File SDB Quicklink button or follow the steps below.

- I. Click on “File / Review Reports” on the navigation bar.
- II. Click on “SDB Participation Reports” on the drop down.
- III. To file a new report, click on the Add New button.
- IV. You will be taken to the instructions page similar to the screenshot below. Please take time to read the instructions.
- V. Click on the Continue button when ready.
- VI. Select the SSR that the report should be associated with.
- VII. Fill out the forms for each step and click “Save & Continue” or “Continue” to move to the next step of the process. *(Note, Click on the context sensitive help button beside the fields for more information)*
- VIII. On step 6, click the Submit button to send the report.
- IX. You may now return to view existing reports to view the status of the report you just entered.

SDB Participation Instructions



 SDB Participation Report (Optional Form 312) [\[show in a separate window\]](#)

New Report

[BACK TO LIST](#)

1 Instructions

2 Enter Contract #

3 Contract Details

4 SDB Participation Report

5 Review

6 Submit Report

SDB Participation by NAICS Industry Subsector Report

Contracts containing the FAR clause at 52.219-25 require the contractor to submit the Optional Form 312 providing a breakdown of subcontracts to small disadvantaged businesses (SDBs) by three-digit NAICS subsector or to submit the same information in their own format.

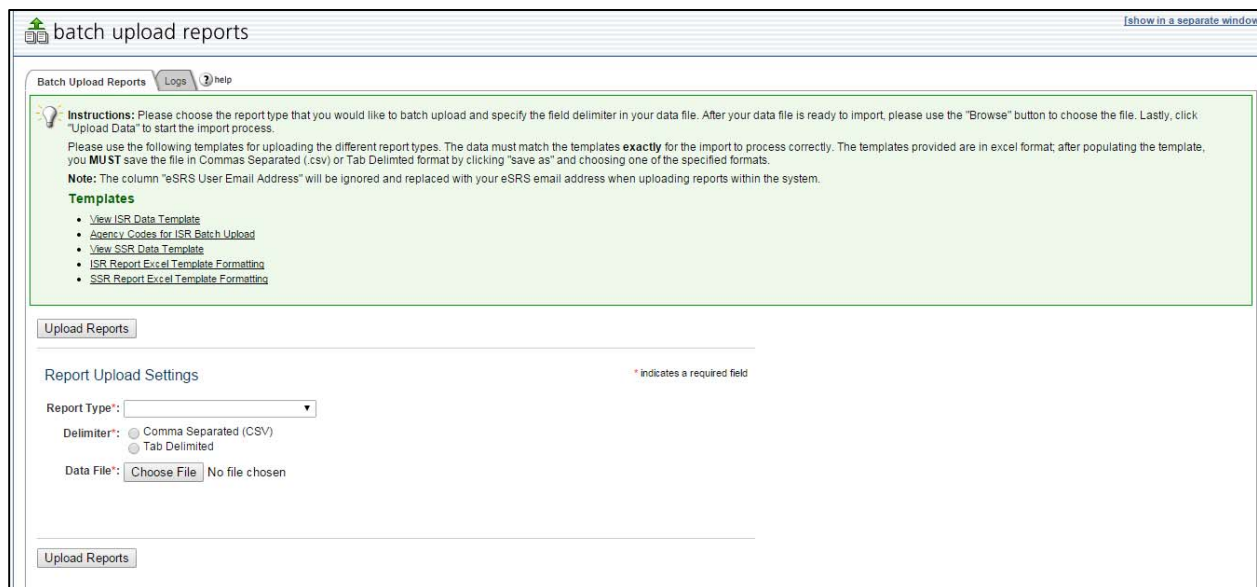
Section 9 Batch Upload Reports

(For Advanced Users Only)

The batch upload capability allows you to upload multiple reports (ISR / SSR) in one template. The template, agency codes and template formatting instructions are provided in the Instructions box.

- I. First download the type of report template you wish to use for batch upload.
- II. Modify the template in Microsoft Excel to include all contracts (ISR) or agencies (SSR) you wish to file for.
- III. Save the excel spreadsheet in a CSV or Tab Delimited file, using the Save As feature in Excel.
- IV. Place the file on a drive where you can access it later.
- V. Enter the Batch Upload Section.
- VI. Choose the Report Type (ISR / SSR)
- VII. Choose the Delimiter
- VIII. Click on Browse, and chose the file that you saved in Step III.
- IX. The file will begin uploading, and will display the result of your upload on screen.

Batch Upload Instructions



batch upload reports [\[show in a separate window\]](#)

Batch Upload Reports [Logs](#) [help](#)

Instructions: Please choose the report type that you would like to batch upload and specify the field delimiter in your data file. After your data file is ready to import, please use the "Browse" button to choose the file. Lastly, click "Upload Data" to start the import process.

Please use the following templates for uploading the different report types. The data must match the templates **exactly** for the import to process correctly. The templates provided are in excel format, after populating the template, you **MUST** save the file in Comma Separated (.csv) or Tab Delimited format by clicking "save as" and choosing one of the specified formats.

Note: The column "eSRS User Email Address" will be ignored and replaced with your eSRS email address when uploading reports within the system.

Templates

- [View ISR Data Template](#)
- [Agency Codes for ISR Batch Upload](#)
- [View SSR Data Template](#)
- [ISR Report Excel Template Formatting](#)
- [SSR Report Excel Template Formatting](#)

Report Upload Settings * indicates a required field

Report Type*:

Delimiter*: ☒ Comma Separated (CSV) ☐ Tab Delimited

Data File*: No file chosen

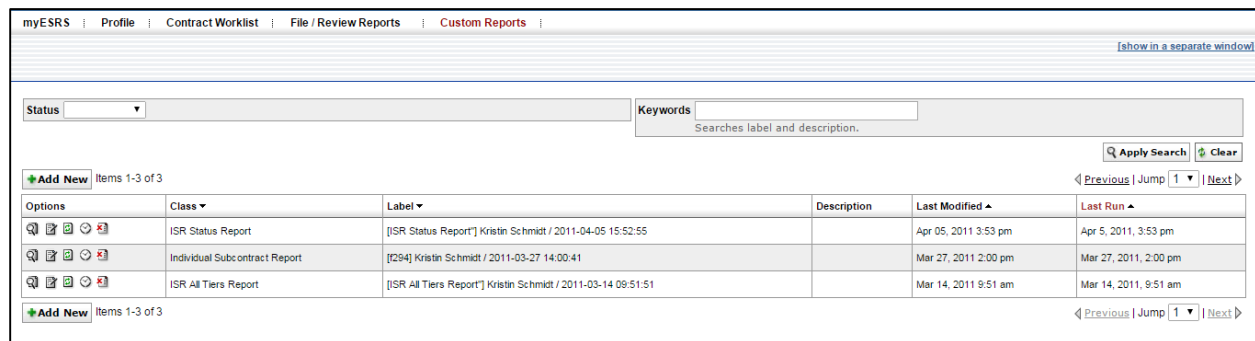
Section 10 Custom Reports













Contractors have been provided with the ability to run ad hoc and pre-defined reports for their organization's contract reporting. Additional information on the Reporting module can be found in the Contractors Generating Reports quick reference guide.

10.1 Build New Reports

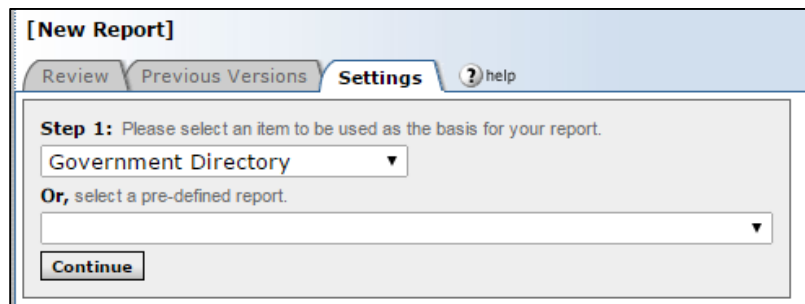
- I. Create New Report by clicking on REPORTING on the left navigation menu.
- II. Click on Add New
- III. You will be taken to a screen similar to the one below.
- IV.

Report Listing



Options	Class	Label	Description	Last Modified	Last Run
   	ISR Status Report	[ISR Status Report] Kristin Schmidt / 2011-04-05 15:52:55		Apr 05, 2011 3:53 pm	Apr 5, 2011, 3:53 pm
   	Individual Subcontract Report	[I294] Kristin Schmidt / 2011-03-27 14:00:41		Mar 27, 2011 2:00 pm	Mar 27, 2011, 2:00 pm
   	ISR All Tiers Report	[ISR All Tiers Report] Kristin Schmidt / 2011-03-14 09:51:51		Mar 14, 2011 9:51 am	Mar 14, 2011, 9:51 am

Add New Report



[New Report]

Review Previous Versions **Settings** help

Step 1: Please select an item to be used as the basis for your report.

Government Directory

Or, select a pre-defined report.

Continue

- V. Select the basis for your report, or choose a predefined report.
- VI. Click Continue
- VII. Before building the report, checkmark the Save As box and input a Name and Description for the Report.
- VIII. When updating an existing report, save the report under a different name by check-marking Copy to New Report.



- IX. Select the fields to be included in the report by check-marking specific fields.
- X. Narrow the focus of the report by clicking on a Filter link under a particular field.
- XI. Once fields and filters have been assigned, view the report by clicking Submit at the bottom of the page. **NOTE: Save & continue will save change to report builder, but will not run report in order to view it.**

The Basis for the reports is broken into two different types of reports, Ad Hoc and Pre-defined.

Ad-Hoc Reports: Can be run based on the user selecting specific filters which will return a specific set of data.

- Individual Subcontract Report**
- Summary Subcontract Report**

Pre-Defined Reports: Can be run at any time and require the user to set specific filters to determine the basis for the report results.

- Subcontracting Contractor Award Dollars**
- Trend Analysis Report**
- Analysis of Subcontracting Plan Goal Attainment**
- Subcontracting Achievements by Federal Agency**
- ISR Status Report**
- SSR Status Report**
- ISR All Tiers Report**
- Time-Phased Individual Subcontract Report**

10.2 View Generated Report

- I. Click on the View Icon beside an existing report. Note: A red “No Data Reported” value indicates that there are no Accepted reports in the system with applicable data.
- II. Show the report in a separate browser by clicking on the Open in New Window button at the top.
- III. Transfer the report into an Excel Workbook by clicking the Save as Excel button.
- IV. Re-configure the report by clicking on Change Settings button at the top.
- V. Go back to the report list by clicking the Return to Report List button.

Review Generated Report

Review Previous Versions Settings ? help																					
regen report		open in new window		save as excel		change settings		return to report list													
Company	SB	SB %	LB	LB %	Total	SDB	SDB %	WOSB	WOSB %	HBCU MI	HBCU MI %	HUBZ	HUBZ %	VOSB	VOSB %	SD_VOSB	SD_VOSB %	ANC	ANC %	ANCN	ANCN %
	26,258,964	36.6	45,493,758	63.4	71,752,722	140,861	0.2	1,417,867	2.0	0	0.0	128,101	0.2	2,168,460	3.0	134,748	0.2	97,707	0.1	0	0.0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4,650,537	62.0	2,851,920	38.0	7,502,457	110,264	1.5	978,986	13.0	0	0.0	0	0.0	2,147,715	28.6	1,685,872	22.5	0	0.0	0	0.0
	141,900	47.3	158,100	52.7	300,000	0	0.0	6,900	2.3	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	12,282	5.7	202,020	94.3	214,302	564	0.3	456	0.2	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0

10.3 View Existing Reports

- I. View Existing Report by clicking on REPORTING on the left navigation menu.
- II. View Saved Queries/Report on the list.
- III. View, Edit, Re-run, View Previous Results by clicking on their respective icons.

View Existing Reports

Reporting [back](#)

Saved Reports [help](#)

Class

Status

Keywords

Searches label and description.

Apply Search



















Clear

Items 1-13 of 13

< Previous

Jump 1

Next >

Options	Class	Label	Description	Last Modified	Last Run
  	Subcontracting Achievements by Federal Agency	[Subcontracting Achievements by Federal Agency"] / 2010-10-06 15:19:44		Sep 15, 2011 2:02 pm	Sep 15, 2011, 2:02 pm
  	Federal Procurement Subcontract Report (SBA Version)	[Federal Procurement Subcontract Report (SBA Version)] / 2011-04-06 12:08:08		Apr 06, 2011 12:08 pm	Apr 6, 2011, 12:08 pm
  	Awards By Contractors, By Service and Type of Business (294)	[Awards By Contractors, By Service and Type of Business (294)] / 2011-02-23 14:41:54		Mar 04, 2011 3:44 pm	Mar 4, 2011, 3:44 pm
  	SSR Status Report	[SSR Status Report"] / 2010-10-18 13:52:52		Nov 15, 2010 4:30 pm	Nov 15, 2010, 4:30 pm
  	Summary Subcontract Report	[f295] / 2010-10-25 11:46:38		Oct 25, 2010 3:57 pm	Oct 25, 2010, 3:57 pm
  	Summary Subcontract Report	[f295] / 2010-10-18 13:49:07		Oct 20, 2010 2:10 pm	Oct 20, 2010, 2:10 pm

A. HISTORIC AND BACKGROUND INFORMATION FOR CORE DISCIPLINES

BUSINESS ADMINISTRATION AND PROJECT MANAGEMENT SUPPORT (Core Discipline 1)

KNOWLEDGE MANAGEMENT (Sub Core Discipline 1.2)

The Chairman Joint Chief of Staff (CJCS) Instruction 5124.01, *Charter of the Knowledge Management Cross-Functional Team* (http://www.dtic.mil/cjcs_directives/cdata/unlimit/5124_01.pdf), defines Knowledge Management as “the process of enabling knowledge flow to enhance a shared understanding, learning, and decision-making. Knowledge flow refers to the ease of movement of knowledge within and among organizations.” To manage, capture, store and reuse knowledge effectively, USCYBERCOM Instruction 5900-01, *Knowledge Management (KM) Program*, identifies four core areas of focus for the command’s KM Program:

- Strategy
- Processes
- Organization and Culture
- Technology

USCYBERCOM’s Chief Knowledge Officer (CKO) is responsible for managing the Knowledge Management program, which includes developing and executing a Knowledge Management strategic plan. The CKO collaborates with the Chief Information Officer (CIO) for the development of Knowledge Management software tools, as Knowledge Management is enabled through the use of key information systems such as online document collaboration.

USCYBERCOM’s Knowledge Management Working Group (KMWG) is charged with amending or initiating policy for Knowledge Management processes, procedures, and technologies. The KMWG ensures that strategic initiatives are coordinated and managed across the Command. All Command personnel have a role in the Knowledge Management process from creation to consumption. The Knowledge Managers are charged with promoting the Knowledge Management best practices within their own organizations and serve as a resource for internal business process design and development. They promote and assist with the use of internal Knowledge Management tools. They should also meet the requirements identified in *Joint Cyberspace Training and Certification Standards (JCT&CS)* for knowledge managers.

Currently, USCYBERCOM uses SharePoint 2010 and 2013 as its Knowledge Management software.

RECORDS MANAGEMENT (Sub Core Discipline 1.3)

The Executive Office of the President Memorandum M-12-18, *Managing Government Records Directive*, 24 August 2012

(<https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>) creates the records management framework and provides for specific actions that will support agency records management programs. DoD 5015.02-STD and DoD 5015.2 STD (2007) define Records

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

Management as "the planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creation, maintenance (use, storage, retrieval), and disposal, regardless of media." Simply stated it is the professional practice or discipline of controlling and governing what are considered to be the most important records of an organization throughout the records life-cycle, which includes from the time such records are conceived, implemented, revised and archived. This work includes identifying, classifying, prioritizing, storing, securing, preserving, retrieving, tracking and archiving of records. The National Archives and Records Administration is responsible for storing permanently valuable historical records.

BUSINESS PROCESS REENGINEERING (Sub Core Discipline 1.4)

Business process reengineering is the practice of rethinking and redesigning processes and workflows by which work is accomplished and products delivered to better support an organization's mission and increase efficiency. Reengineering starts with a high-level assessment of the organization's mission, strategic goals, and customer needs. Then current processes are identified along with areas where gaps may exist.

LOGISTICS (Sub Core Discipline 1.5)

JP 1-02 ([http://www.dmrta.army.mil/documents/jp1_02\[1\].pdf](http://www.dmrta.army.mil/documents/jp1_02[1].pdf)) defines logistics as "planning and executing the movement and support of forces." It further defines logistics support as "support that encompasses the logistic services, materiel, and transportation required to support the continental U.S. based and worldwide deployed forces. JP 4.0 defines the core logistics functions "The core logistic functions are: deployment and distribution, supply, maintenance, logistic services, operational contract support, engineering, and health services." The core logistic functions are considered during the employment of U.S. military forces in coordinated action toward a common objective and provide global force projection and sustainment.

CYBER OPERATIONS (Core Discipline 2)

JP 3-0 (http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf) *Joint Operations*, provides that "USCYBERCOM is a sub-unified command subordinate to the U.S. Strategic Command (USSTRATCOM) and directs the operations and defense of specified DoD information networks. It is capable of conducting full-spectrum military cyberspace operations to enable U.S. freedom of action in cyberspace and enable actions in other domains and deny the same to our adversaries. Cyberspace operations is the employment of cyberspace capabilities primarily to achieve objectives in or through cyberspace." JP 3-12, *Cyberspace Operations* (http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf) defines a cyberspace capability as "a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."

Section 18(d)(3) of the Unified Command Plan expands upon the above delegated USCYBERCOM responsibilities by also including the specific missions of providing shared situational awareness of cyberspace operations, including indications and warning; integration and synchronization of cyberspace operations with CCMDs and other appropriate U.S.

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

Government agencies tasked with defending the nation's interests in cyberspace; and providing support to civil authorities and international partners.

USCYBERCOM categorizes cyberspace operations into three areas: OCO, DCO, and DODIN Operations. JP 3-12 (http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf) defines these terms as:

Offensive Cyberspace Operations (OCO): “Cyberspace operations intended to project power by the application of force through cyberspace.”

Defensive Cyberspace Operations (DCO): “Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.”

DoD Information Network (DODIN) Operations: “Operations to design, build, configure, secure, operate, maintain, and sustain DoD networks to create and preserve information assurance on the DODIN.” Defending the DODIN includes ensuring the security objectives of confidentiality, integrity, and availability are maintained at a level commensurate with the criticality and sensitivity of the DODIN.

CYBERSPACE PLANNING (Core Discipline 3)

Joint Planning consists of planning activities associated with joint military operations by combatant commanders and their subordinate joint force commanders in response to contingencies and crisis. It transforms national strategic objectives into activities by development of operational products. Joint plans and orders are developed with the strategic and military end states in mind. The commander and planners derive their understanding of those end states from strategic guidance. Specifically in this domain, commanders integrate cyberspace capabilities at all levels and in all military operations. Depending on the level of planning being conducted (Deliberate, Crisis Action, Future Operations (FuOps), Operations, and Execution), plans should address how to effectively integrate cyberspace capabilities, counter an adversary's use of cyberspace, secure mission critical networks, operate in a degraded environment, efficiently use limited cyberspace assets, consolidate requirements for cyberspace capabilities, and assess the ability of the DoDIN to support offensive and defensive operations.

Planning translates strategic guidance and direction into campaign plans, level 1-4 plans, and operation orders. Joint operation planning may be based on defined tasks identified in the Global Employment of Forces (GEF) and the Joint Strategic Capabilities Plan (JSCP). Alternatively, joint operation planning may be based on the need for a military response to an unforeseen current event, emergency, or time-sensitive crisis. Joint operation planning encompasses a number of elements, including three broad operational activities, four planning functions, and a number of related products.

USCYBERCOM develops plans and orders through the application of operational art and operational design and by using the Joint Operation Planning Process (JOPP). Deliberate planning encompasses the preparation of plans that occur in non-crisis situations. It is used to

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

develop campaign and contingency plans for a broad range of activities. Crisis Action Planning (CAP) is a process for getting vital decision-making information available up the chain of command to the President and Secretary of Defense. CAP encompasses the activities associated with the time-sensitive development of Operations Orders (OPORDs) for the deployment, employment, and sustainment of assigned, attached, and allocated forces and capabilities in response to a situation that may result in actual military operations.

USCYBERCOM employs each of the steps of deliberate planning and CAP through operational design and using JOPP for planning activities as a supported and supporting command through established Joint Planning Groups (JPGs), Operational Planning Groups (OPGs), and Operational Planning Teams (OPTs). Cyberspace operations planning activities are coordinated through the Integrated Joint Special Technical Operations (IJSTO) and Review and Approval Process for Cyberspace Operations (RAPCO) processes.

ALL-SOURCE INTELLIGENCE (Core Discipline 4)

Intelligence is a joint function integral to all military operations. Joint Publication (JP) 2-01 (http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf) defines combatant command (CCMD) roles in joint intelligence activities as “assisting the commander and staff in developing strategy, planning major operations and campaigns, coordinating the intelligence structure and architecture, recommending appropriate command relationships for intelligence, surveillance, and reconnaissance assets, and supervising the production and dissemination of appropriate intelligence products.” USCYBERCOM’s role in intelligence activities includes all-source intelligence support to the development of cyberspace operations capabilities planning, integration, coordination and execution. Intelligence activities assist operations and planning processes in the development of mission objectives.

Intelligence collection is conducted in response to specific needs expressed by policy makers and military commanders for information. Intelligence and operation activities collaborate to ensure all intelligence collection requirements are identified as early as possible.

CAPABILITY MANAGEMENT AND DEVELOPMENT (Core Discipline 5)

Capability Management and Development includes development efforts for near term integration, science and technology (S&T) efforts to push technological limits to generate breakthroughs in engineering disciplines; and Research and Development (R&D) efforts which focuses on the development of new or improved capabilities of proven science and technology to the point they are appropriate for operational use. Test and evaluation is part of capability development and determines if a capability is appropriate for operational use. USCYBERCOM capability management and development efforts are conducted with the goal to fulfill tactical, operational, and strategic requirements, and to develop quick reaction cyberspace capabilities. USCYBERCOM provides the strategic vision and direction for R&D and S&T across the Services.

Capability Management and Development efforts are conducted by USCYBERCOM to advance concepts and technologies. USCYBERCOM works with the services, industry, academia, the IC

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

and the DoD labs to bring new ideas and tools forward in support of the Cyber Mission Forces (CMF) in the shortest time possible. USCYBERCOM leverages this pool of expertise to build diverse capabilities to enable full-spectrum military operations. USCYBERCOM also enforces a process to ensure there is no redundancy of effort and that multiple DoD entities can use the same capabilities when possible to maximize returns on investment. The cyber forces train on, and integrate those capabilities in their tactical training exercises. Capability development for the national and CCMD cyber mission forces aligns with USCYBERCOM's three mission areas of defending the nation; secure, operate, and defend the DODIN; and provide support to CCMDs.

CYBER TRAINING (Core Discipline 6)

Historically, annually, in FY2013 approximately 120 training classes were held, in FY2014 approximately 450 classes, and in FY2015 approximately 630 USCYBERCOM classes and approximately 1110 classes related to J7 projects. The majority of classes were held in the Washington, DC metropolitan area. Approximately 20 percent of classes were held outside of the Washington, DC metropolitan area.

CYBER EXERCISES (Core Discipline 6)

USCYBERCOM is an integrated part of the government process for national event responses. Therefore, to remain in a state of readiness, the Command participates in exercises that demonstrate coordination of response actions and coordination across government organizations, departments, and agencies in response to various cyber scenarios. USCYBERCOM plans and trains for major cyber incidents.

USCYBERCOM exercises put operating concepts to the test during the exercise continuum of Cyber Knight, Cyber Guard, and Cyber Flag. These exercises are designed to train and certify CMF teams and can consist of exercises, conventional maneuvers and kinetic fires in conjunction with cyber operations. Current Cyberspace related exercise (support required subject to change during the Period of Performance):

- *Cyber Knight*: Validates certification and proficiency standards against the CMF teams in accordance with the USCYBERCOM T&R Manual.
- *Cyber Flag*: Coupled with Joint Doctrine and the Force Model, includes all the Service Cyber components as well as inter-agency and international partners. Provides realistic training for the cyber components and government organizations in executing cyber defense and offense operations across the full spectrum of operations against simulated adversary forces. Provides the opportunity to apply new and developing tactics, techniques, and procedures for the cyber mission force and coalition teams.
- *Cyber Guard*: Coupled with Joint Doctrine, the Force Model is a whole-of-government event exercising state- and national-level responses to adversary actions against critical infrastructures in a virtual environment. This exercise promotes shared awareness and coordination to mitigate and recover from an attack while assessing potential federal cyber responses.

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

- Cyber Wargames apply modeling and simulation techniques to look five years into the future, and include expert participation from industry and academia. The objectives of wargames are to explore potential cyber environments and impacts on cyber operations, identify policy and coordination requirements needed to operate in the cyber realm, and identify cyber tools and capabilities necessary to conduct cyber operations from Intelligence, Surveillance, and Reconnaissance (ISR) through operations to Battle Damage Assessment (BDA) in the cyber environment. Wargames contribute to the development of exercise plans used in Cyber Flag.
- Table Top Exercises (TTXs) provide support for the planning and execution of exercises. TTXs validate requirements through each phase in order to validate that scenarios can be carried out and function as predicted in the planning process.

INFORMATION TECHNOLOGY (IT)/COMMUNICATIONS (COMMS) (Core Discipline 7)

IT/Comms is defined as the engineering, development and use of technology to enhance and support the USCYBERCOM environment. The USCYBERCOM help desk is included in the support to the USCYBERCOM environment. Supporting the USCYBERCOM environment encompasses the planning and implementation of hosting solutions for capabilities, and the maintenance of technology solutions. Currently, the programs/languages in use in the environment are as follows: HTML, JAVA, and CSS.

As the CMF is established in accordance with Joint Staff guidance, capability development should occur concurrently to ensure the CMF have the requisite facilities, platforms, equipment, and tools needed to accomplish their assigned mission. USCYBERCOM develops and maintains the strategy for identifying the mix of alternative scalable platforms required to meet operational requirements, both for steady state and contingency purposes. USCYBERCOM plays a role coordinating operational and technical requirements to ensure interoperability for CMF and compatibility with mission infrastructures.

INTEGRATED TECHNOLOGY (Sub Core Discipline 7.1)

Currently, the service desk supports approximately 1,200 users and is manned 10x5. Weekend on call requested to alternate with uniformed personnel.

CYBERSECURITY (Sub Core Discipline 7.3)

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. USCYBERCOM strives for robust, resilient, and defensible networks and architectures by establishing and encouraging adherence to cybersecurity standards.

The cybersecurity risk management process will ensure U.S. interests, DoD operational capabilities, and DoD individuals, organizations, and assets are appropriately protected from

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

known vulnerabilities, adversarial activities, and improperly configured/non-compliant security controls. This process will be accomplished by protecting DoD assets from known vulnerabilities, threats, unauthorized adversary access to sensitive information, unauthorized disclosure/release of sensitive information, improper storage/use, disruption/modification of data, or conditions that would negatively affect the confidentiality, integrity, and availability of the cyberspace environment.

STRATEGY/POLICY/DOCTRINE DEVELOPMENT AND CAMPAIGN ASSESSMENTS (Core Discipline 8)

In accordance with the *DoD Strategy for Operating in Cyberspace*, USCYBERCOM, along with its mission partners and allies, assist the DoD in building doctrine and concepts for operating in cyberspace. Doctrine will define and organize the technical command and control of DoD cyber elements, and address the fundamental principles that guide the employment of cyber mission forces in coordinated action toward common objectives, and include the TTPs. USCYBERCOM, in conjunction with the DoD and the Intelligence Community, informs policy and resourcing decisions.

USCYBERCOM strategy initiatives will foster unity of effort and action to operate effectively in cyberspace, and outline activities that can achieve success in cyberspace operations.

USCYBERCOM strategy will advance the nation's security posture in cyberspace, and provide for synchronization of various cyber elements, as well as international partners, allies, and industry.

USCYBERCOM coordinates and collaborates on cyber related strategy, policy and doctrine from higher headquarters and reports on evolving cyberspace policy trends and issues in with the U.S. Government.

Policies will provide course of action statements of guidance in pursuit of USCYBERCOM objectives.

Campaign assessments provide an analytical appraisal of how past activities contributed to progress toward campaign objectives and assist the commander in determining whether campaign plans should be refined, adapted, terminated, or continued without modification. Assessment results may identify shortfalls in strategy, policy, and/or resources and provide the analysis to underpin associated recommendations for changes. USCYBERCOM conducts deliberate campaign assessments on a semi-annual basis to support CDRUSCYBERCOM as well as in support of USSTRATCOM's campaign plan 8000.

ENGAGEMENT ACTIVITIES (Core Discipline 9)

Strategic engagements create opportunities for coordination and collaboration with partners across the U.S. Government, private sector, academia, and foreign allies to share information, promote responsible behavior, and defend U.S. interests in cyberspace. Engagements, whether through words, images, or actions, encourage the understanding of the scope and scale of threats and the risk and responsibilities stakeholders in cyberspace together share. Operationalized

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

engagements strengthen collective cybersecurity with partners through the sharing of threat and vulnerability information, advancement of defensive capabilities, development of resiliency, and support of a deterrent posture.

USCYBERCOM cultivates partnerships across the U.S. Government to ensure DoD mission assurance, deter or defeat strategic threats to U.S. interests and infrastructure, and achieve Joint Force commander objectives. USCYBERCOM, together with the National Security Agency (NSA) and the Defense Information Systems Agency (DISA), maintains key partnerships across the DoD, Department of Homeland Security (DHS), and Department of Justice, Department of State, CCMDs, and other U.S. Departments and Agencies. These partnerships enable whole-of-government engagement and unified strategic communications to support U.S. deterrence strategy and policy in cyberspace.

USCYBERCOM engages with foreign allies and partners to deter shared threats and increase international security through our commitment to an open, secure, interoperable, and reliable Internet. USCYBERCOM collaborates and coordinates with foreign allies and partners to improve warning capabilities, collective defense, and capability and capacity building. Foreign partner engagements include training and exercises, planning and operations, and information sharing to deter and effectively respond to malicious cyberspace activity.

USCYBERCOM also engages with the private sector and academia to increase our collective knowledge and publicize malicious cyberspace activities. USCYBERCOM relies on the private sector and academia for technological and conceptual innovation, reliable and secure infrastructure, supporting services and expertise, and research and development to improve U.S. technical capabilities, ensure information assurance, and defend the nation's vital interests in cyberspace.

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

B. REFERENCES: Below is a list of documents that are referenced in the Request for Proposal and this Attachment.

- CJCSI 5124.01. 12 April 2013. “*Charter of the Knowledge Management Cross-Functional.*”
http://www.dtic.mil/cjcs_directives/cdata/unlimit/5124_01.pdf
- CJCSI 3500.01G. 15 March 2012. “*Joint Training Policy and Guidance for the Armed Forces of the United States.*”
 - www.dtic.mil/doctrine/training/cjcsi3500_01g.pdf
- DoD April 2015. “*The Department of Defense Cyber Strategy.*”
http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- DoD 5015.2-STD. 25 April, 2007. *Electronic Records Management Software Applications Design Criteria Standard*
 - www.dtic.mil/whs/directives/corres/pdf/501502std.pdf
- DoD Manual 5200.01 Volumes (1–4). 24 February 2012. “*Information Security Program.*”
 - *Volume 1: Overview, Classification, and Declassification*
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
 - *Volume 2: Marking of Classified Information*
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
 - *Volume 3: Protection of Classified Information*
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf
 - *Volume 4: Controlled Unclassified Information (CUI)*
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf
- DoD Directive 5205.07. 1 July 2010. “*Special Access Program (SAP) Policy.*”
 - <http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf>
- DoDI 8500.01. 14 March 2014. “*Cybersecurity.*”
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
- DoDI 8510.01. 12 March 2014. “*Risk Management Framework (RMF) for DoD Information Technology (IT).*”
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
- DoD 8570.01M. 19 December 2005. “*Information Assurance Workforce Improvement Program.*” www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
- The Executive Office of the President Memorandum M-12-18, *Managing Government Records Directive*, 24 August 2012.
<https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>
- Joint Chiefs of Staff Joint Publication 1-02. 15 March 2012. “*Department of Defense Dictionary of Military and Associated Terms.*”
[http://www.dmrta.army.mil/documents/jp1_02\[1\].pdf](http://www.dmrta.army.mil/documents/jp1_02[1].pdf)
- Joint Chiefs of Staff Joint Publication 2-0. 22 October 2013. “*Joint Intelligence.*”
http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf
- Joint Chiefs of Staff Joint Publication 2-01. 05 January 2012. “*Joint and National Intelligence Support to Military Operations.*”
http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf

ATTACHMENT Q – CURRENT ENVIRONMENT AND BACKGROUND

- Joint Chiefs of Staff Joint Publication 3-0. 11 August 2011. “*Joint Operations.*”
http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf
- Joint Chiefs of Staff Joint Publication 3-12. 5 Feb 2013. “*Cyberspace Operations,*”
http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
- Joint Chiefs of Staff Joint Publication 4-0. 16 October 2013. “*Joint Logistics.*”
http://www.dtic.mil/doctrine/new_pubs/jp4_0.pdf
- Joint Chiefs of Staff Joint Publication 5-0. 11 August 2011. “*Joint Operation Planning.*”
http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf
- Secretary of the United States Air Force. 15 July 2010. “*Cyberspace Operations: Air force Doctrine Document 3-12.*”
<http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf>
- Unified Command Plan, Section 18(d)(3)
- U.S Cyber Command Policy Memorandum 2013-01
- USCYBERCOM Instruction 5900-01, *Knowledge Management (KM) Program,*
- The White House. May 2011. “*U.S. International Strategy for Cyberspace.*”
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- USCYBERCOM 5200-08 Requirements Management Process
- USSTRATCOM's Campaign Plan 8000

Labor Categories	KEYW Composite Rate - Base Year	KEYW Composite Rate - Option 1	KEYW Composite Rate - Option 2	KEYW Composite Rate - Option 3	KEYW Composite Rate - Option 4	KEYW Ceiling Rate - Base Year	KEYW Ceiling Rate - Option 1	KEYW Ceiling Rate - Option 2	KEYW Ceiling Rate - Option 3	KEYW Ceiling Rate - Option 4
Escalation Factor										
Administrative Specialist - I										
Administrative Specialist - II										
Administrative Specialist - III										
Business Process Engineer - I										
Business Process Engineer - II										
Business Process Engineer - III										
Collection Manager - I										
Collection Manager - II										
Collection Manager - III										
Configuration Manager - I										
Configuration Manager - II										
Configuration Manager - III										
Cybersecurity Developer - I										
Cybersecurity Developer - II										
Cybersecurity Developer - III										
Cybersecurity Engineer - I										
Cybersecurity Engineer - II										
Cybersecurity Engineer - III										
Cybersecurity Network Architect - I										
Cybersecurity Network Architect - II										
Cybersecurity Network Architect - III										
Cyberspace Analyst - I										
Cyberspace Analyst - II										
Cyberspace Analyst - III										
Cyberspace Fires (Targets) Analyst - I										
Cyberspace Fires (Targets) Analyst - II										
Cyberspace Fires (Targets) Analyst - III										
Cyberspace Intelligence Analyst - I										
Cyberspace Intelligence Analyst - II										
Cyberspace Intelligence Analyst - III										
Cyberspace Joint Operation Planner - I										
Cyberspace Joint Operation Planner - II										
Cyberspace Joint Operation Planner - III										
Cyberspace Operations Engineer - I										
Cyberspace Operations Engineer - II										
Cyberspace Operations Engineer - III										
Cyberspace Policy Analyst - I										
Cyberspace Policy Analyst - II										
Cyberspace Policy Analyst - III										
Cyberspace Scientist - I										
Cyberspace Scientist - II										
Cyberspace Scientist - III										
Cyberspace Training Facilitator - I										
Cyberspace Training Facilitator - II										
Cyberspace Training Facilitator - III										

(b) (4)

Labor Categories	KEYW Composite Rate - Base Year	KEYW Composite Rate - Option 1	KEYW Composite Rate - Option 2	KEYW Composite Rate - Option 3	KEYW Composite Rate - Option 4	KEYW Ceiling Rate - Base Year	KEYW Ceiling Rate - Option 1	KEYW Ceiling Rate - Option 2	KEYW Ceiling Rate - Option 3	KEYW Ceiling Rate - Option 4
Escalation Factor	(b) (4)									
Cyberspace Training Specialist - I	(b) (4)									
Cyberspace Training Specialist - II	(b) (4)									
Cyberspace Training Specialist - III	(b) (4)									
Graphic Artist - I	(b) (4)									
Graphic Artist - II	(b) (4)									
Graphic Artist - III	(b) (4)									
Graphic Designer - I	(b) (4)									
Graphic Designer - II	(b) (4)									
Graphic Designer - III	(b) (4)									
Information Technology Specialist - I	(b) (4)									
Information Technology Specialist - II	(b) (4)									
Information Technology Specialist - III	(b) (4)									
Inspector General Specialist - I	(b) (4)									
Inspector General Specialist - II	(b) (4)									
Inspector General Specialist - III	(b) (4)									
Intelligence Planner - I	(b) (4)									
Intelligence Planner - II	(b) (4)									
Intelligence Planner - III	(b) (4)									
Knowledge Management Specialist - I	(b) (4)									
Knowledge Management Specialist - II	(b) (4)									
Knowledge Management Specialist - III	(b) (4)									
Legislative Affairs Specialist - I	(b) (4)									
Legislative Affairs Specialist - II	(b) (4)									
Legislative Affairs Specialist - III	(b) (4)									
Malware Analyst - I	(b) (4)									
Malware Analyst - II	(b) (4)									
Malware Analyst - III	(b) (4)									
Modeling & Simulation Engineer - I	(b) (4)									
Modeling & Simulation Engineer - II	(b) (4)									
Modeling & Simulation Engineer - III	(b) (4)									
Network Engineer - I	(b) (4)									
Network Engineer - II	(b) (4)									
Network Engineer - III	(b) (4)									
Open Source Analyst - I	(b) (4)									
Open Source Analyst - II	(b) (4)									
Open Source Analyst - III	(b) (4)									
Operational Design Cognitive Operator - I	(b) (4)									
Operational Design Cognitive Operator - II	(b) (4)									
Operational Design Cognitive Operator - III	(b) (4)									
Operations Research Analyst - I	(b) (4)									
Operations Research Analyst - II	(b) (4)									
Operations Research Analyst - III	(b) (4)									
Program Manager - I	(b) (4)									
Program Manager - II	(b) (4)									
Program Manager - III	(b) (4)									

Labor Categories	KEYW Composite Rate - Base Year	KEYW Composite Rate - Option 1	KEYW Composite Rate - Option 2	KEYW Composite Rate - Option 3	KEYW Composite Rate - Option 4	KEYW Ceiling Rate - Base Year	KEYW Ceiling Rate - Option 1	KEYW Ceiling Rate - Option 2	KEYW Ceiling Rate - Option 3	KEYW Ceiling Rate - Option 4
Escalation Factor	(b) (4)									
Project Analyst - I	(b) (4)									
Project Analyst - II	(b) (4)									
Project Analyst - III	(b) (4)									
Project Manager - I	(b) (4)									
Project Manager - II	(b) (4)									
Project Manager - III	(b) (4)									
Public Affairs Specialist - I	(b) (4)									
Public Affairs Specialist - II	(b) (4)									
Public Affairs Specialist - III	(b) (4)									
Records Management Specialist - I	(b) (4)									
Records Management Specialist - II	(b) (4)									
Records Management Specialist - III	(b) (4)									
SharePoint Developer - I	(b) (4)									
SharePoint Developer - II	(b) (4)									
SharePoint Developer - III	(b) (4)									
SIGINT Policy Analyst - I	(b) (4)									
SIGINT Policy Analyst - II	(b) (4)									
SIGINT Policy Analyst - III	(b) (4)									
Software Developer - I	(b) (4)									
Software Developer - II	(b) (4)									
Software Developer - III	(b) (4)									
Special Security Officer Specialist - I	(b) (4)									
Special Security Officer Specialist - II	(b) (4)									
Special Security Officer Specialist - III	(b) (4)									
Subject Matter Expert - I	(b) (4)									
Subject Matter Expert - II	(b) (4)									
Subject Matter Expert - III	(b) (4)									
Systems Administrator - I	(b) (4)									
Systems Administrator - II	(b) (4)									
Systems Administrator - III	(b) (4)									
Systems Engineer - I	(b) (4)									
Systems Engineer - II	(b) (4)									
Systems Engineer - III	(b) (4)									
Systems Integrator - I	(b) (4)									
Systems Integrator - II	(b) (4)									
Systems Integrator - III	(b) (4)									
Technical Writer - I	(b) (4)									
Technical Writer - II	(b) (4)									
Technical Writer - III	(b) (4)									
Test Engineer - I	(b) (4)									
Test Engineer - II	(b) (4)									
Test Engineer - III	(b) (4)									
Web Development - I	(b) (4)									

IDIQ Contract# GS000Q16AJD0004

USCYBERCOM Support Contract

in support of:

**United States Cyber Command
(USCYBERCOM)**



Issued to:

**KEYW Corporation
7740 Milestone Parkway, Suite 150
Hanover, MD 21076**

Conducted under FAR Part 15

Issued by:

**The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405**

**May 20, 2016
FEDSIM Project Number AF00753**

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

This contract is established under Federal Acquisition Regulation (FAR) Part 15 as part of a Multiple Award, Indefinite Delivery, Indefinite Quantity (MA-IDIQ) to support the United States Cyber Command (USCYBERCOM). The contractor shall provide all management, supervision, labor, facilities, and materials necessary to perform on a Task Order (TO) basis. Hereafter, this USCYBERCOM IDIQ contract will be referred to as the Basic Contract while TOs issued under the Basic Contract will be referred to as individual TOs. The TOs shall be performed in accordance with (IAW) all sections of the Basic Contract.

An acronym listing to support the Basic Contract is included in Section J (Attachment L).

B.1.1 CONTRACT TYPES

The USCYBERCOM Basic Contract is an MA-IDIQ contract for services based requirements in support of USCYBERCOM, and is available for use by the Cyber Mission Force (CMF), Service Cyber components, and Joint Force Headquarters (JFHQs).

The Basic Contract allows for all contract types at the TO level (e.g., Cost-Reimbursement (all types), Fixed-Price (all types), Time-and-Materials (T&M), and Labor-Hour (LH)). TOs may also combine more than one contract type (e.g., Firm-Fixed-Price (FFP)/Cost, FFP/LH etc.). Additionally, TOs may include incentives, performance-based measures, multi-year or option periods, and commercial or non-commercial items.

B.1.2 MINIMUM GUARANTEE AND MAXIMUM CEILING

The guaranteed minimum for each awarded Basic contract is \$2,500. The maximum dollar ceiling for each individual TO placed under the Basic Contract is \$300,000,000. There is no limit to the number of TOs that may be placed under this Basic Contract. The maximum dollar ceiling for this Basic Contract is \$710,000,000.

B.2 PRICES/COSTS

The Contractor shall furnish all personnel, material, services, and facilities to perform the requirements set forth in the Basic Contract.

B.2.1 TASK ORDER PRICING

The Basic Contract provides the Ordering Contracting Officer (CO) the flexibility to determine fair and reasonable pricing tailored to the TO requirement dependent upon level of competition, risk, uncertainties, complexity, urgency, and contract type. The Ordering CO has the authority and responsibility for the determination of cost or price reasonableness for each TO's requirements. Adequate price competition at the TO level, in response to a Task Order Request (TOR), is the preferred method of establishing fair and reasonable pricing.

The Ordering CO must identify the applicable contract type for all Contract Line Item Numbers (CLINs) in each individual TO.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.2.2 LABOR RATES

B.2.2.1 BURDENED LABOR RATE

The term “burdened labor rate” is defined as the technical, management, and support staff required to complete tasking on a project, along with appropriate load factors, and exclusive of any profit or fee.

B.2.2.2 LOADING FACTORS

The loading factors are those defined in the Contractor’s forward pricing rates, and include such items as overhead, fringe, general and administration (G&A), or any other elements of cost.

B.2.2.3 CEILING RATES

The term “Ceiling Rates” represents the maximum direct labor rates to be proposed and/or billed under this Contract. These ceiling direct labor rates apply to cost-reimbursable orders and proposals for fixed-price orders.

Ceiling rates do not govern T&M and LH TO proposals, as ceiling rates do not include fee/profit. However, ceiling rates will be used in the evaluation of T&M/LH TO proposals.

The ceiling rate should anticipate the maximum technical expertise needed over the life of the contract and is not necessarily bound by current staff. See Section B.3

B.2.2.4 COMPOSITE RATES

The term “composite rate” is defined as the average burdened hourly labor rate experienced by the Contractor for similar scope of work and shall be based on current personnel in labor category descriptions in Section J (Attachment B). See Section B.3

The composite rate is the average rate based on current staff and similar tasking.

B.2.2.5 SUBCONTRACTOR RATES

Subcontractor rates will be negotiated separately as TO awards require.

B.2.3 CONTRACT TYPES

B.2.3.1 FIXED-PRICE TASK ORDERS

Fixed price is defined under Federal Acquisition Regulation (FAR) Subpart 16.2, Fixed-Price Contracts.

B.2.3.2 COST-REIMBURSEMENT TASK ORDERS

Cost Reimbursement is defined under FAR Subpart 16.3, Cost-Reimbursement Contracts. FAR Part 30, Cost Accounting Standards Administration and FAR Part 31, Contract Cost Principles and Procedures, may apply to cost-reimbursement TOs.

The contractor shall have and maintain an acceptable accounting system that will permit timely development of all necessary cost data in the form required by the proposed contract type.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

The contractor may be required to submit a cost proposal with supporting information for each cost element, including, but not limited to, direct labor, fringe benefits, overhead, general and administrative (G&A) expenses, facilities capital cost of money, other direct costs, and fee consistent with its cost accounting system, provisional billing rates, forward pricing rate agreements, and/or Cost Accounting Standards (CAS).

Cost Reimbursement TOs shall only be used for the acquisition of non-commercial items.

B.2.3.3 INCENTIVE TASK ORDERS

Incentives are defined under FAR Subpart 16.4, Incentive Contracts.

B.2.3. TIME AND MATERIALS (T&M) AND LABOR HOUR (LH) TASK ORDERS

T&M and LH are defined under FAR Subpart 16.6, T&M and LH Contracts.

The contractor may provide separate and/or blended loaded hourly labor rates for prime contractor labor, each subcontractor, and/or each Division, Subsidiary, or Affiliate in accordance with the provisions set forth in FAR 52.216-29, Defense Federal Acquisition Regulation Supplements (DFARs) 252.216-7002, FAR 52.216-30, or FAR 52.216-31 at the TO level. The CO must identify which provision is applicable in the TO solicitation, and the contractor must comply with the provision.

T&M and LH TOs require the USCYBERCOM standardized labor categories and their associated rates to be identified in the TO proposal and award document.

Ancillary subcontract labor shall be proposed and awarded as Materials in accordance with FAR 52.232-7, Payments under Time-and-Materials and Labor-Hour Contracts.

B.3 BASIC CONTRACT ESTABLISHED SCHEDULE RATES

The Basic Contract includes the standard set of labor categories in Section J (Attachment B). The contractor's awarded composite and ceiling are hereby incorporated and made a material part of this contract. See the following table labeled KeyW IDIQ Basic Contract Rates.

The awarded Basic Contract labor rates are established as "composite and ceiling rates" as defined within Sections B.2.2.3 and B.2.2.4. The ceiling rates contain the fully burdened hourly rates for work performed at any location within the US including Alaska and Hawaii excluding profit/fee. Additionally, the ceiling rates are the maximum rates that will be invoiced at the TO level when billing against the Basic Contract labor categories and being invoiced by the prime in accordance with Section G of this contract.

(b) (4)

A large black rectangular redaction box covers the content of the table referenced in the text. The text "(b) (4)" is written in red to the left of the box.

Profit and Fee will be negotiated at the individual TO level.

B.4 INDIRECT RATES

Indirect rates include, but may not be limited to, indirect material handling rates, overhead rates, and G&A rates.

SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

B.5 LONG DISTANCE TRAVEL

Long Distance Travel required in the performance of TOs issued under this contract shall be reimbursed at actual cost in accordance with the limitations set forth in FAR 31.205-

46. Profit/fee shall not be applied to travel costs. Unless otherwise directed by TO terms and conditions, the contractor may apply indirect costs to long distance travel consistent with the contractor's approved accounting practices.

Local travel will not be reimbursed under TOs issued against the contract.

The Ordering CO must identify a not-to-exceed (NTE) long distance travel ceiling under a separate CLIN on the TO.

B.6 TOOLS AND ODCS

Tools and ODCs acquired under this contract will be on a cost-reimbursable basis. Unless otherwise directed by individual TO terms and conditions, the contractor may apply indirect costs and fee to Tools and ODCs consistent with the contractor's approved accounting practices.

B.7 SUBCONTRACTING

Subcontractor rates will be negotiated separately as TO awards require.

For non-commercial items, subcontracting shall follow the procedures set forth in FAR Part 44, Subcontracting Policies and Procedures. For commercial items, subcontracting shall follow the procedures set forth in FAR Part 12, Acquisition of Commercial Items.

SECTION C – DESCRIPTION OF WORK

C.1 BACKGROUND

On June 23, 2009, the Secretary of Defense directed the Commander of US Strategic Command (USSTRATCOM) to establish a sub-unified command, USCYBERCOM. The newly established USCYBERCOM developed a mission to plan, coordinate, integrate, synchronize, and conduct activities to: direct the operations and defense of specified Department of Defense (DoD) information networks (DODIN) and prepare to, and when directed, conduct full spectrum military Cyberspace Operations in order to enable actions in all domains.

USCYBERCOM is charged with accomplishing the following:

- a. Unifying existing cyberspace resources, creating synergy that does not currently exist, and synchronizing war-fighting effects to defend the information security environment
- b. Centralizing command of cyberspace operations in order to strengthen DoD cyberspace capabilities and integrate and bolster the DoD's cyber expertise
- c. Improving the DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace
- d. Supporting the Armed Services' ability to confidently conduct high-tempo, effective operations, as well as, protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.

USCYBERCOM accomplishes this by organizing supporting forces to achieve unity of effort across three lines of effort: protect and defend US cyberspace interests, project power in and through cyberspace, and partner with interagency and partner nations. Each line of effort is applied to three mission objectives: deter or defeat strategic threats to U.S. interests and infrastructure, ensure DoD mission assurance, and achieve Joint Force Commander objectives.

C.1.1 USCYBERCOM MISSION

USCYBERCOM conducts and synchronizes activities to: secure, operate, and defend the DODIN; attain freedom of action in cyberspace while denying same to adversaries; and, when directed, conduct full spectrum cyberspace operations in order to deter or defeat strategic threats to U.S. interests and infrastructure, ensure DoD mission assurance, and achieve Joint Force Commander objectives.

C.1.2 CURRENT ENVIRONMENT

Background information relating to each of the task areas below is detailed in Section J, Attachment Q.

“The 2015 DoD Cyber Strategy” provides additional background information related to the current strategic goals and objectives of USCYBERCOM.

C.1.3 JOINT DIRECTORATES

USCYBERCOM is comprised of 10 J-Directorates; their functions are as follows:

J0 - Chief of Staff: Provides enterprise-level staff leadership, strategic communications coordination, logistics requirements, Command information, business management, support, and enabling functions.

SECTION C – DESCRIPTION OF WORK

J1 - Manpower & Personnel: Leads the Command in creating an integrated, agile, responsive, and ready cyber workforce capable of conducting full spectrum Cyberspace Operations.

J2 - Intelligence: Provides decision-quality, timely all-source intelligence which informs and enables USCYBERCOM across the full spectrum of military Cyberspace Operations.

J3 - Operations: Plans, coordinates, integrates, synchronizes, and conducts activities directing the operation and defense of the DODIN and, when directed, conducts full spectrum military Cyberspace Operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to our adversaries.

J4 - Logistics: Provides integrated logistics capabilities enabling USCYBERCOM and components to achieve desired global effects.

J5 - Plans and Policy: Responsible for cyberspace strategies, policies, doctrine, deliberate plans, assessments, and partnerships.

J6 - Command and Control (C4) Systems and Information Technology (IT): Provides premier C4 and IT capabilities for USCYBERCOM to conduct full spectrum military Cyberspace Operations.

J7 - Joint Exercises and Training: Develops and prepares world-class fully capable cyber forces for the present and future, ready to conduct military operations, build partner capacity, and promote engagement through doctrine, education, training, exercises, simulation, wargames, and readiness.

J8 - Capability and Resource Integration: Guides the Planning, Programming, Budgeting, and Execution (PPBE) process in acquiring resources to satisfy mission requirements. Provides procurement and financial management services for effective expenditure of funding. Conducts analyses and assessments to ensure investments are balanced to achieve maximum benefit.

J9 - Advanced Concepts and Technology: Drives delivery of Tactics, Techniques, and Procedures (TTPs) and corresponding material capability solutions designed to meet USCYBERCOM and Combatant Command (CCMD) cyberspace requirements across full spectrum Cyberspace Operations.

C.2 SCOPE

The scope of this contract includes services and associated tools needed to support USCYBERCOM's mission. It is a broad scope of cyberspace support services including new and emerging technologies which will evolve over the life of the contract.

The scope of these requirements includes capabilities, knowledge, and expertise in the full range of technologies, Cyberspace Operations, joint operation planning, training and exercises, and business areas needed to support USCYBERCOM's operational mission, which extends throughout the CMF, Service Cyber Components, and JFHQs. In addition, the scope includes all-source intelligence, research and development, test, and evaluation services.

These services may be required throughout the United States, its territories and possessions and in foreign countries.

SECTION C – DESCRIPTION OF WORK

C.3 OBJECTIVE

The objective of this requirement is an IDIQ contract dedicated to providing mission support services to USCYBERCOM, CMF, Service Cyber Components, and JFHQs. These required core disciplines include the following:

- a. Business Area Support and Project Management
- b. Cyberspace Operations
- c. Cyberspace Planning
- d. All-Source Intelligence
- e. Capability Management and Development
- f. Cyberspace Training and Exercises
- g. Information Technology (IT)/Communications (COMMS)
- h. Strategy/Policy/Doctrine Development and Campaign Assessments
- i. Engagement Activities
- j. Security

C.4 CORE DISCIPLINES

The following describes the services required for each core discipline. The specific support requirements will be the subject of fully defined TOs that will be executed and administered in accordance with the terms and conditions defined in the Basic Contract and TO. The evolving responsibilities of USCYBERCOM may require additional support for responding to cyber events that are not known at this time. High quality products and services delivered in a timely and cost-effective manner will be the primary criteria for the work performed under the Basic Contract. The specific application of these criteria will be supplied with the individual TOs. All core disciplines within the scope of this Basic Contract and at the individual TO level require coordination and collaboration with other contractors in order to be performed effectively. Particularly in the case of responding to a specific threat, all personnel involved, including contractors, will be integrated to produce results quickly. Quick response times required to counter threats are unique to the domain of warfare and require tightly coupled integration for mission success. The following core disciplines are vital to enabling USCYBERCOM mission success.

C.4.1 CORE DISCIPLINE 1 – BUSINESS AREA SUPPORT AND PROJECT MANAGEMENT SUPPORT

The business area support core discipline is defined as support to enable an efficient and effective work environment within and across all Directorates, including Government, military, and contractor personnel, and with JFHQs subordinate headquarters, Service Cyber Components, CCMD, components and agencies with cyber-related missions.

C.4.1.1 SUB CORE DISCIPLINE 1 – ADMINISTRATIVE SUPPORT

Administrative Support includes general office support; coordination between organizations for day-to-day operations; scheduling and coordinating meetings, visits, conferences, and events;

SECTION C – DESCRIPTION OF WORK

preparing, processing, and tracking correspondence; preparing meeting minutes and meeting notes; preparing briefings; conducting data collection and reporting; conducting workflow/project tracking; and tracking action items. The Government also requires support for providing specialized administrative support in offices throughout USCYBERCOM such as the Command Section, Public Affairs Office, Records Management Office, Publications Management Office, Knowledge Management Office, and the History Office.

Administrative Support also includes providing support to cyber exercise planning conferences including Joint Worldwide Planning Conference, Joint Event Life Cycle (JELC) planning conferences (Concept Development Conference, Initial Planning Conference, Main Planning Conference, Final Planning Conferences), and Master Scenario Events List (MSEL) Development Conference. Conference design, facilitation, and analysis also fall under this core discipline.

This sub core discipline includes support providing routine administrative and clerical assistance, such as receiving/screening telephone calls and visitors. For example, support includes, but is not limited to, the following:

- a. Responding to routine, non-technical requests for information; scheduling appointments; making arrangements for conferences, meetings, and presentations, including location, schedule, and agenda; and coordinating all other arrangements with staff/participants
- b. Providing specialized Administrative Support to USCYBERCOM Joint Directorates, organizations and special staff offices such as the Legislative Affairs Office, Public Affairs Office, Command Secretariat, Command Engagements/Visits, Inspector General, and the Commander's Action Group
- c. Assisting with office procedures, Command protocol, correspondence, messages, reports, forms, filing, mail, training, travel security, personnel procedures, and preparation for office moves
- d. Composing routine/non-technical correspondence and preparing reports, and making content contributions and corrections to internal Command administrative/clerical correspondence or other appropriate subjects
- e. Providing support to initiate travel arrangements, complete travel orders, and prepare vouchers for Command leadership
- f. Preparing PowerPoint presentations in support of management briefings

Supporting this core discipline may require contractors to work within Government-provided software packages with emphasis on the Defense Travel System, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft SharePoint 2010, 2013, and later upgrades or additional software based upon the requirements in individual TOs.

Support for this core discipline also includes providing administrative and clerical expertise to support the achievement of operations and research objectives, information analysis, exercise and training development, and implementation of training objectives. For example, support includes maintaining Microsoft SharePoint and shared file locations for knowledge management of documentation and office-related information. This core discipline also includes providing administrative support for exercise and training design, planning, preparation, execution,

SECTION C – DESCRIPTION OF WORK

analysis, evaluation, and reporting; Joint Training Plans and After-Actions Programs development; and individual, team, and collective mission area training.

Administrative Support services may also include providing administrative coordination activities for obtaining spaces to accommodate meetings, working groups, events, conferences, conference support, materials required to support such events, and the IT and audio/visual/video teleconferencing (VTC) services and equipment that may be needed at the unclassified, secret, and top secret (TS) levels.

C.4.1.2 SUB CORE DISCIPLINE 2 – KNOWLEDGE MANAGEMENT

Knowledge Management support services include providing technical expertise to support USCYBERCOM Directorates and the Chief Knowledge Officer (CKO) to formulate and implement Knowledge Management strategies, policies, processes and procedures to enable USCYBERCOM to create, share, and maintain records in accordance with the DoD Knowledge Management Policy requirements.

DoD Knowledge Management services also include the maintenance and utilization of Knowledge Management communication and collaboration tools to capture, reuse, and transfer Command knowledge efficiently and effectively. Knowledge Management support will be required across all network domains. Additional background information is provided in Section J (Attachment Q).

C.4.1.3 SUB CORE DISCIPLINE 3 – RECORDS MANAGEMENT

The contractor shall provide Records Management support in accordance with the Executive Office of the President Memorandum M-12-18, *Managing Government Records Directive*, 24 August 2012, DOD 5015.02-STD, and DOD 5015.2-STD (2007). For example, this support shall include identifying, prioritizing, storing, securing, preserving, retrieving, tracking, and archiving records. Additional background information is provided in Section J, Attachment Q.

Records Management is defined as providing technical expertise to support the formulation of Records Management strategies and policies to enable USCYBERCOM to create and maintain records in accordance with the DoD Record Management Policy requirements and to document the roles and responsibilities of USCYBERCOM in the conduct of its mission. Furthermore, Records Management includes assisting the Chief of Command Secretariat, Command Publications Manager, and several directorates within USCYBERCOM with the development and maintenance of a Command Publications Library as appropriate on the three network domains. Support shall include accounting for work product history in conjunction with the record.

C.4.1.4 SUB CORE DISCIPLINE 4 – BUSINESS PROCESS REENGINEERING

Business Process Reengineering is defined as providing Enterprise Business Transformation expertise, including Lean Six Sigma and Process Change Management methodology, to support the CKO in analyzing current USCYBERCOM workflows and processes to identify process inefficiencies and areas of improvement, reduce redundancy, and re-engineer applicable processes to increase efficiency. Additional background information is provided in Section J, Attachment Q. This core discipline includes, but is not limited to, the following services:

SECTION C – DESCRIPTION OF WORK

- a. Developing approaches for improving organizational performance and the activities needed to implement new or revised business or functional processes arising from business process reengineering undertakings
- b. Identifying the necessary development and/or integration of IT to enable improvements in processes
- c. Providing technical expertise to ensure approved solutions to re-engineer processes are implemented and their effectiveness is measured against current processes
- d. Revising performance measures in alignment with new business processes

C.4.1.5 SUB CORE DISCIPLINE 5 – LOGISTICS

Logistics support is defined as providing Logistics planning and management expertise for obtaining and managing facility and space requirements, as well as the supply and the planning and executing movements of materials and the transportation required. Logistics includes obtaining offsite facilities as needed for the conduct of crisis action planning, simultaneous planning events, cyber event management, and planning for periods of non-disruption and continuity of operations. Additional background information is provided in Section J, Attachment Q.

The support for this core discipline includes providing management logistical oversight for facility management and asset management. This support includes utilizing existing Government proprietary systems/protocols for automation purposes of asset management and equipment tracking within Government-owned Sensitive Compartmented Information Facilities (SCIFs) in the local travel area and within satellite facilities. For example, logistics support includes, but is not limited to, the following:

- a. Providing support in management of Government-owned SCIFs in multiple locations
- b. Managing the flow of resources between the point of origin, procurement, configuration management, and through disposal, to include purchasing, handling, controlling, and transportation of material and other property
- c. Maintaining proper retention of logs, files, and supporting documentation for all movement of materials
- d. Communicating and coordinating with all parties involved in materials movements

Support for this core discipline includes assisting the Government in managing the development of upgrades and system improvements, tracking and reporting material, establishing and maintaining material handling procedures, and providing asset management, configuration management, and scheduling. Logistics Support also includes developing and managing power/space/cooling requests, and Baseline Exemption Requests (BERs). The contractor's Logistics Support shall adhere to and be provided in accordance with Federal and DoD policy.

C.4.1.6 SUB CORE DISCIPLINE 6– PROJECT ANALYSIS

Project Analysis is defined as providing technical expertise to assist with the following Project Analysis functions to ensure proper and efficient execution and performance of programs, and that capabilities are successfully developed and acquired to meet USCYBERCOM's requirements. These requirements include, but are not limited to, the following:

SECTION C – DESCRIPTION OF WORK

- a. Tracking and analyzing the status of programs fulfilling USCYBERCOM requirements for remaining within scope, within budget, and on schedule, while mitigating risks
- b. Maintaining program information and status of ongoing program activities
- c. Analyzing and refining initial user needs and assist in defining requirements
- d. Analyzing validated and prioritized requirements to manage timelines and risks
- e. Assisting with validating and prioritizing requirements
- f. Collaborating with teams managing related and dependent requirements to maintain status of collective progress
- g. Supporting execution and delivery of capabilities to end-users
- h. Providing lifecycle support to close out capability development and implementation
- i. Analyzing project risks and developing risk mitigation plans
- j. Developing courses of action to fulfill gaps and requirements
- k. Conducting analysis of programs, managing deliverables, and preparing graphs, tables, diagrams, and presentations to present analysis conclusions and recommendations

Project Analysis support is also defined as assisting the USCYBERCOM with proper and efficient execution of programs, requirements identification and definition, and course of action development for the integration, management, and sustainment of Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) capabilities, and efforts to secure, operate, and defend the DODIN.

Project Analysis support includes, but is not limited to, providing support to prepare, review, and update program documentation and status in support of milestone decisions, leadership, and external reviews. Project Analysis support also includes assisting with organizing and preparing for program meetings and conferences.

Project Analysis support includes preparing white papers, graphs, tables, diagrams, and briefings to present analysis conclusions and recommendations. Support for the Project Analysis core discipline also includes, but is not limited to, the following:

- l. Developing methods for tracking program performance and refining project analysis processes, methods, and tools
- m. Maintaining program plans and coordinating with the program managers to ensure programs fulfill requirements upon delivery
- n. Developing and maintaining program files in accordance with records management processes

C.4.1.7 SUB CORE DISCIPLINE 7 – PROJECT MANAGEMENT

Project Management support is defined as assisting in the management of the project's scope, schedule, budget, and manage risk to ensure the accomplishment of project goals, as well as providing TO Project Management. Support includes, but is not limited to, developing project documentation, risk management documentation, plans, and project schedules. Project Management support includes tracking project status in Government-approved formats,

SECTION C – DESCRIPTION OF WORK

evaluating operational and technical alternatives, and performing risk assessments. Support also includes identifying the project critical path and risk mitigation strategies.

Project Management support includes, but is not limited to, the following:

- a. Developing work breakdown structures and integrated master schedules
- b. Preparing charts, tables, graphs, and diagrams to assist in analyzing problems, project risks, and issues, and preparing project management plans, project documentation, and reports
- c. Coordinating schedules to facilitate completion of contract deliverables, briefings/presentations, and project reviews; performing analysis; and developing and reviewing project administrative operating procedures

C.4.2 CORE DISCIPLINE 2 - CYBERSPACE OPERATIONS

Cyberspace Operations support is defined as providing technical expertise to assist in the planning, coordination, and synchronization of OCO and DCO, and operation of the DODIN. Additional background information is provided in Section J (Attachment Q). At TO award, the Government will provide information concerning the training, format of the forms, and appropriate use of the tools, roles, and reporting procedures.

Cyberspace Operations support is also defined as providing technical expertise during the conduct of assessments of Cyberspace Operations, including the development and deliberate comparison of forecasted outcomes with actual events utilizing Measures of Effectiveness (MOE) and Measures of Performance (MOP) when determining progress toward desired end-states and satisfying objectives. Support for this core discipline includes participating in and contributing to the development of the Joint Operations Center (JOC) Emergency Action Procedures in preparedness to defend the nation through inter-agency emergency cyber procedures. Support for this core discipline shall also entail surge support in the occurrence of a crisis action matter. The surge support shall participate in activities to respond to a crisis action matter and unknown cyber threats. The duration of surge support during the period of performance may or may not be determined by USCYBERCOM at the time of occurrence.

Cyberspace Operations support also includes:

- a. Assisting in providing maneuver, fires, and effects through the application of capabilities in and through the cyberspace domain
- b. Supporting USCYBERCOM in the creation and dissemination of orders and directives to provide guidance to the DoD
- c. Conducting critical and technical research and analysis to define Commander's Critical Information Requirements (CCIR), Priority Intelligence Requirements (PIR), and Essential Elements of Friendly Information (EEFI) for reporting cybersecurity incidents
- d. Contributing technical expertise to develop TTPs for conducting Cyberspace Operations, measures, and countermeasures and supporting their implementation
- e. Developing and implementing incidence reporting, event handling, and secure configuration guidance to protect, mitigate, and remediate service outages and adversarial activities; and assisting with USCYBERCOM's efforts in the DoD and whole

SECTION C – DESCRIPTION OF WORK

of Government by contributing to the development of policies, doctrine and processes, courses of action, the Situational Awareness Report (SAR), and input for the National Defense Authorization Act (NDAA) 935 report

- f. Providing assistance and input to the maneuver, fires, and effects planning process through the application of capabilities in and through the cyberspace domain

Services that are included in the Cyberspace Operations core discipline also include providing technical expertise to assist in fulfilling USCYBERCOM's responsibilities to the Joint Information Environment (JIE) initiative by identifying requirements and Concept of Operations (CONOPS) that focus on the execution of DODIN Operations and DCO-IDM, in addition to assisting in the development, synchronization, integration, and assessment of operational standards in support of achieving the JIE end-state.

C.4.3 CORE DISCIPLINE 3 - CYBERSPACE PLANNING

Cyberspace Planning support is defined as providing comprehensive strategic operational planning support to USCYBERCOM. This includes organizing the work of the Commander, staff, subordinate/supporting Commanders and partners to develop effective plans and orders; synchronizing planning for Cyberspace Operations in coordination with other combatant Commanders, the Services, and others as directed; transforming national strategic objectives into activities; and providing options, identifying resources, and identifying and mitigating risks. It also includes efforts to plan, manage, and integrate the USCYBERCOM and Cyber National Mission Force (CNMF) joint exercise and training programs and after-action processes to achieve and sustain USCYBERCOM mission-essential task proficiency. Additional background information is provided in Section J (Attachment Q).

Support for this core discipline includes, but is not limited to, providing in-depth deliberate planning expertise, planning support during rapidly developing situations, and plans and orders development for current and future operations. It also includes supporting USCYBERCOM in the development of policy, plans, processes, procedures, and governing directives for securing, operating, and defending the DODIN and projection of power through cyberspace. The contractor shall provide input to address shortfalls, prioritize and validate requirements, and be prepared to modify development planning efforts based on the changing cyberspace environment.

- a. **Deliberate Planning** includes the management and implementation of the Adaptive Planning Process from strategic guidance to completion of USCYBERCOM level one through level four contingency plans, synchronization of USCYBERCOM's missions into plans through internal and external collaboration, and coordination with all mission partners. Deliberate Planning encompasses the preparation of plans that occur in non-crisis situations.
- b. **Crisis Action Planning** is defined as providing technical input and content recommendations to assist in short-term crisis action plans through internal and external collaboration and coordination with all mission partners. Support includes assisting with Crisis Action Planning and the development of all orders and plans to meet time-sensitive event horizons.
- c. **Future Operations Planning** is defined as providing technical input and content recommendations to assist in future operations plans through internal and external

SECTION C – DESCRIPTION OF WORK

collaboration and coordination with all mission partners. Support includes assisting with Future Operations Planning and the development of all orders and plans to meet mid-range time horizons.

- d. **Joint Operational Planning** support includes, but is not limited to, providing technical expertise to assist with the development of operational plans that contain a variety of viable cyberspace options, including following the Joint Operation Planning Process (JOPP) of planning initiation, mission analysis, courses of action (COA) development, COA analysis war gaming, COA comparison and approval, and plan or order development.
- e. **National Mission Team/Execution Planning** support includes, but is not limited to, providing technical and joint planning expertise to assist with the development of tactical joint operational plans in coordination with higher headquarters, mission partners, and tactical teams. Support for this functional area also includes assisting with future operations and mission planning for the development of tactical-level plans and execution of orders.
- f. **Joint Exercise and Training Planning** support includes, but is not limited to, comprehensive strategic planning support to USCYBERCOM to plan, manage, and integrate the USCYBERCOM and CNMF joint exercise and training programs and after-action processes to achieve and sustain USCYBERCOM mission-essential task proficiency.

C.4.4 CORE DISCIPLINE 4 – ALL-SOURCE INTELLIGENCE

All-Source Intelligence analysis is defined as support for planning efforts, from strategic to the tactical level. This discipline area shall include conducting research and analysis, collection management, indications and warning, targeting, imagery analysis, signals intelligence analysis, joint intelligence preparation of the battlespace, and crisis planning to standing and deployed cyberspace forces engaged in operations. Additional background information is provided in Section J (Attachment Q). Support for this core discipline includes, but is not limited to, screening All Source Intelligence reporting, accessing and summarizing evaluated and previously unevaluated information, discriminating threat information from All Source Intelligence into actionable intelligence, and disseminating warning and threat analysis for real-world contingencies. Support also includes researching all source reporting to produce predictive and current finished intelligence products and coordinating all analytical products and support national level organizations and theater staffs for dissemination across tactical, operational, and strategic environments. All-Source Intelligence support also includes communicating factual information clearly and concisely, both orally and in writing, often under pressure and tight deadlines.

Services in support of All-Source Intelligence include, but are not limited to, the following:

- a. Analyzing All Source Intelligence information to produce assessments, reports, articles, threat analyses, special studies etc., responsive to user needs, and complying with suspense dates for draft and final products
- b. Maintaining all source databases on area of responsibility, and using multiple source intelligence tools to perform all source threat force analysis

SECTION C – DESCRIPTION OF WORK

- c. Analyzing and fusing reports from multiple intelligence sources (Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT), Open Source) to provide intelligence preparation of the battlespace, target development, and early warning of emerging threats
- d. Screening and researching all source reporting, accessing and summarizing previously unevaluated information, and discriminating threat information into actionable intelligence
- e. Monitoring all sources of intelligence to ensure adequacy of coverage and timeliness of assessments, and tasking incoming Requests for Information (RFIs) to appropriate cyberspace division
- f. Identifying intelligence gaps and requesting solutions via collections process

C.4.5 CORE DISCIPLINE 5 - CAPABILITY MANAGEMENT AND DEVELOPMENT

Capability Management and Development is defined as providing technical assurance, engineering and architecture analysis, and research for the creation and updating of system architectures' initial capability documents, capability development documents, capability production documents, and engineering guidance documents (standards, specifications, technical architectures, systems). Additional background information is provided in Section J (Attachment Q). Support for this core discipline includes conducting tests and evaluations to support the analysis and testing of cyber-related capabilities.

Tasks in support of Capability Management and Development include, but are not limited to, the following:

- a. Researching, developing, demonstrating, integrating, and testing innovative technology in support of cyberspace threat defense and management in an effort to facilitate proactive development and testing of cyberspace offensive and defensive capabilities
- b. Evaluating and validating sensor system performance capabilities and effectiveness, assessing risk, and determining operational feasibility and benefits of USCYBERCOM's systems or technology prototypes, to include recommending assessments of system performance, identifying deficiencies, and investigation of physical science phenomena
- c. Providing IT support and performing studies, analyses, and experimentation in both laboratory and non-laboratory environments. When supporting Research, Development, Test, and Evaluation (RDT&E) tasks, the contractor shall address, at minimum, any life cycle phase(s) and include science and technology efforts.
- d. Evaluating unproven technology applications, identifying potential risks, and documenting and submit results in support of evaluation findings
- e. Providing drawing support services
- f. Participating in technical reviews and meetings in support of capability management and development activities

Support for this core discipline also includes providing technical expertise and collaborating with USCYBERCOM and its partners to identify and capture capability development requirements. Service in support of this core discipline includes developing artifacts for capability development

SECTION C – DESCRIPTION OF WORK

requirements, including white papers and CONOPs. Support for Capability Management and Development also includes providing technical expertise and participating in activities to identify courses of action for fulfilling capability development requirements, and collaborating with stakeholders to determine the best course of action. Support also includes conducting requirements decomposition and requirements elicitation activities for capability development efforts. Services to be supported also include, for example, providing technical expertise during participation in program reviews to ensure the capability development program is fulfilling the requirement.

Additional tasks in support of Capability Management and Development include, but are not limited to, the following:

- g. Supporting the capability management and development process by coordinating with Intelligence Community (IC) tool developers, the CMF tool developers, and other weapon/tool/capability providers and submitting data on cyber capabilities, and reviewing, analyzing, and maintaining data provided by end users and developers on operational cyber capabilities and associated data
- h. Conducting cyber capability analysis to pair operational requirements with cyber capabilities
- i. Providing technical input for the development of requirements and support the development of both offensive and defensive cyberspace capabilities to achieve USCYBERCOM goals, and for achieving situational awareness and a common operating picture of activities happening in cyberspace
- j. Supporting the Government in providing situational awareness of cyber incidents, health, performance, availability, and reliability of the DODIN

C.4.6 CORE DISCIPLINE 6 – CYBERSPACE TRAINING AND EXERCISES

Cyberspace Training and Exercises support is defined as providing technical expertise for the development and assessment of Cyberspace Training and Exercise programs. These programs provide for and enhance the quality for, and of, the Cyber Forces in support of command mission objectives. Cyberspace Training and Exercises also includes supporting the creation of sustainable, repeatable training programs to meet this demand. Additional background information is provided in Section J (Attachment Q).

Services in support of the Cyberspace Training and Exercises discipline include providing comprehensive cyber training and exercise support for USCYBERCOM to plan, manage, conduct, and integrate the cyber training and exercise programs. This includes identifying, tracking, and resolving issues impacting training, exercises, and daily operations. Services in support of this core discipline also include assisting in the analysis of training requirements in order to ensure that both individual members and cyber teams are adequately trained and prepared to maintain the requisite level of readiness.

C.4.6.1 SUB CORE DISCIPLINE 1 – CYBERSPACE TRAINING

Support of the Cyberspace Training sub core discipline includes assisting in the analysis of the training curriculum, performance objectives, training plans, certification standards, exercise objectives, and evaluation standards. For example, as part of the analysis, contractors shall

SECTION C – DESCRIPTION OF WORK

project future performance objectives and assist with the development of training plans and materials to support Joint Cyber Training objectives in order to ensure Command personnel possess the necessary skills required to accomplish their missions.

Services that are included in support of the Cyberspace Training sub core discipline include, but are not limited to, the following:

- a. Providing facilitators and instructors for cyberspace curriculum planning, development, scheduling, delivery, assessment, evaluation, and maintenance
- b. Assisting in preparing instructors to facilitate USCYBERCOM training requirements, coordinating with, and assisting in preparing, Government instructors and guest speakers for delivery of curriculum training modules, and preparing materials for course delivery
- c. Developing and maintaining joint standards and assessing and documenting readiness of individuals, teams, and units against joint standards
- d. Assessing training curriculum and courses to ensure an emphasis on the application of skill with opportunities for students to demonstrate the attainment of the learning objectives
- e. Developing and integrating updates to the curriculum. Requirements for updates will come as a result of feedback from student evaluations as well as Government input, or the contractor's suggested alterations.
- f. Preparing to support Mobile Training Teams (MTT) that will be utilized to instruct curriculum for an average of a two-week period. Coordinate MTT training schedules, locations, instructors, and course materials.
- g. Assisting with continuous performance improvement and standardization efforts based on future capabilities needs, alternate approaches, flexible applications, and adversary modifications
- h. Assisting in the maintenance of training requirements to ensure accuracy and timeliness of records
- i. Assisting in the training waiver process through facilitation of the process and coordination with individuals for completeness of documentation
- j. Assisting with maintaining training schedules, enrollments, and associated travel plans
- k. Assisting with and conduct cyber training across USCYBERCOM to support the cyber training program
- l. Creating call out messages (e.g., CONOPs and Orders) for Government review and processing
- m. Developing COAs in response to training objectives
- n. Assisting with facilitating the establishment of training environments to includes a next-generation CMF Persistent Training Environment (PTE)
- o. Designing, developing, and maintaining registration websites, and portals providing course information and materials

SECTION C – DESCRIPTION OF WORK

C.4.6.2 SUB CORE DISCIPLINE 2 – CYBERSPACE EXERCISES

The Cyberspace Exercises, war games, and Table Top Exercises (TTXs) that occur regularly throughout every fiscal year are anticipated as follows:

Type of Event	Estimated Number of Events per year	Average Number of Participants
Team Certification Events	9	50-60
CCMD Exercise Support	10-15	20-60
Cyber Knight or similar	9	50-60
Cyber Flag or similar	3 (2 mini & 1 full)	Mini = 50-60/Full = 800
Cyber Guard or similar	5 (4 mini and 1 full)	Mini = 50-60/Full = 500
Cyber Wargame	3	150
TTX	25	15-30

Cyberspace exercises support is defined as analyzing outputs stemming from USCYBERCOM exercises and supporting the development, architecture, and infrastructure capabilities of persistent training and test environments. Support for this sub core discipline includes providing technical input for the development of requirements of training and test environments including the physical infrastructure and facilities.

Services in support of this sub core discipline include, but are not limited to, collaborating with Command elements to implement objectives, priorities, and plans for the USCYBERCOM joint exercise program. Support also includes contributing to the development of exercises utilizing inputs from the Cyberspace Operations Planning process, and to focus on Joint Mission Essential Tasks (JMETs) for known and anticipated operational missions, capabilities, and improving of Command processes through lessons learned. Cyberspace Exercises shall simulate alternative operational scenarios and provide insights into how issues may play out in the real world and the real cyber world.

Services in support of the Cyberspace Exercises sub core discipline include providing research, analysis, and recommendations to conceive, develop, execute, and support Joint Event Lifecycle events including CCMD exercises, tabletop exercises, and scenario development/synchronization. Each year, USCYBERCOM will determine which CCMD exercises it will support.

Services in support of the Cyberspace Exercises sub core discipline include providing technical expertise and participating in the lifecycle events of conducting an exercise which include, but is not limited to, the following:

- a. Incorporating CCMD Training Objectives and/or Cyberspace Training Objectives into exercises, and participating in concept development conference/meetings
- b. Providing comprehensive cyber exercise support to USCYBERCOM to plan, manage, and integrate the USCYBERCOM and CNMF joint exercise and training programs and after-action processes to achieve and sustain USCYBERCOM mission-essential task proficiency

SECTION C – DESCRIPTION OF WORK

- c. Contributing to the development of Certification and Proficiency Standards, which are required for each of the CMF teams
- d. Designing, developing, and maintaining registration websites and portals providing exercise information and materials
- e. Participating in all phases of the JELC, including assisting with the development of objectives, storylines and themes, CONOPs, development of exercise scenarios, guidance documentation, rules of engagement, MSEL, exercise design documents, exercise orders and directives, supporting plans, exercise schedule, and exercise control plans
- f. Participating in, and refining materials that result from the initial planning, mid-planning, and final planning conferences.
- g. Participating in exercise hosting and system support activities, and coordinating the selection, acquisition, and accountability of hardware, software, and necessary software licenses for exercise execution. Contributing to the development of exercise floor-plans to include equipment, network, and floor plan design.
- h. Participating in the execution of exercises, including blue team/white cell participation
- i. Conducting exercise analysis, evaluation, review, assessment, after-action reporting
- j. Conducting post-exercise lessons learned studies and incorporate these in future exercises
- k. Providing technical expertise for the continuous development and refinement of exercises, wargames, and TTXs design constructs and concepts in order to continuously identify future manpower, organizational, technical, policy, and procedural requirements for the cyber environment

C.4.7 CORE DISCIPLINE 7 – INFORMATION TECHNOLOGY (IT)/ COMMUNICATIONS (COMMS)

The requirements for supporting the USCYBERCOM environment encompass the planning and implementation of hosting solutions for capabilities and the maintenance of technology solutions. Additional background information is provided in Section J (Attachment Q).

C.4.7.1 SUB CORE DISCIPLINE 1 - INTEGRATED TECHNOLOGY

Integrated Technology support is defined as providing technical expertise for the planning and engineering of enterprise architectures management, system configuration, system administration support, and system engineering support. Additional background information is provided in Section J (Attachment Q).

Examples of services in support of (ISO) the Integrated Technology sub core discipline include, but are not limited to, following:

- a. Performing specialized tests to support analysis and evaluation of technologies and systems
- b. Conducting test and evaluation planning; preparation, logistical, and transportation planning; prototype assessments in field environments; operating test instrumentation; and supporting remote testing, war game seminars, and capstone events

SECTION C – DESCRIPTION OF WORK

- c. Providing network, systems, and software engineering, analysis of system concepts, system design and interoperability, and providing recommendations for optimization
- d. Identifying and contributing to the development of IT/COMMS requirements, and provide expertise for determining the best course of action to fulfill IT/COMMS requirements. For example, the contractor shall be required to review and analyze development, production, and system support plans as well as participate in program reviews and make evaluations of technical performance and progress.
- e. Assisting the Government in the preparation of technical documents, specifications, and requirements for developmental projects, and making trade-off/best technical approach analyses. Examples of deliverables that shall be prepared are as follows: System Engineering Plans (SEPs), design plans, technical reports, and engineering studies.

Integrated Technology services also include providing comprehensive IT/COMMS support to USCYBERCOM to plan, manage, and integrate the USCYBERCOM and CNMF joint exercise and training programs and after-action processes to achieve and sustain USCYBERCOM mission-essential task proficiency. For example, the contractor shall provide technical assistance and data and information management for analysis, coordination, planning, execution, and after-action reporting.

An additional service in support of this sub core discipline includes, but is not limited to, providing technical expertise to support joint architectural and systems engineering analysis to validate that proposed Command, Control, Communications, and Computers (C4) designs can be fully integrated with existing, projected, and targeted Information System (IS) enterprise architectures, and that they facilitate effective communications and authorized exchange of information. This is to ensure effective implementation of Cyberspace Operations employed by multiple DoD program community partners and the synchronization of DoD CIO policy directives with the operational community.

An additional example of the support required under this core discipline includes providing technical expertise and participate in JIE working groups, systems, and network engineering activities, and providing analysis and input to the architecture development efforts supporting JIE and JFHQ–DODIN (e.g., JIE Operations Center Reference Architecture).

Furthermore, support of this sub core discipline, includes performing the technical and administrative management of USCYBERCOM's Enterprise IT Service Desk. To ensure non-disruptive and secure operation of USCYBERCOM's Enterprise IT, the contractor shall serve as a point of contact in managing and responding to USCYBERCOM customer requests for IT support, and provide systems administration, configuration management, and web development support to USCYBERCOM web-based initiatives and functions in accordance with mission requirements.

SECTION C – DESCRIPTION OF WORK

C.4.7.2 SUB CORE DISCIPLINE 2 – ASSET MANAGEMENT AND PURCHASING

Asset Management and Purchasing is defined as conducting vendor research and analysis and recommend IT equipment that best meet USCYBERCOM requirements. In addition, support for this sub core discipline is defined as initiating, facilitating, and participating in the IT purchasing process for acquiring and integrating IT/COMMS materials.

Services that are required under this Asset Management and Purchasing core discipline include, but are not limited to, the following:

- a. Coordinating the receipt of materials and accounting for the inventory of IT/COMMS materials, as well as confirming assets assigned to the contractor on a recurring 90-day basis
- b. Initiating the processes and obtaining requisite permissions for introducing new materials into the network. For example, the contractor shall coordinate with required parties and conduct network preparation activities for introducing new materials into the network.
- c. Remaining cognizant of license agreements and license expiration dates and conducting activities for their increase or decrease of users, renewal, or termination of program use. In addition, the contractor shall remain cognizant of spare equipment and initiate the IT purchasing process to ensure a spare part inventory.

C.4.7.3 SUB CORE DISCIPLINE 3 - CYBERSECURITY

This core discipline is defined as providing Cybersecurity in accordance with the implementation of DODI 8140.01 (August 11, 2015), and DODI 8510.01 (March 12, 2014), Risk Management Framework (RMF) for DoD IT, when determining whether to integrate a new capability into the existing infrastructure. Additional background information related to this core discipline is provided in Section J (Attachment Q).

Services required ISO the Cybersecurity core discipline include, but are not limited to, the following:

- a. Providing Cybersecurity expertise to identify/analyze vulnerabilities, determine threats, and assess risk to the DODIN
- b. Providing Cybersecurity technical input during the planning, development, and implementation of capabilities to secure, operate, and defend the DODIN
- c. Conducting analyses of assets, facilitating partner collaboration for situational awareness, and validating compliance of DoD security controls and policies
- d. Providing Cybersecurity input in the strategic, operational, and tactical planning, coordination, and synchronization of OCO, DCO, and DODIN operations
- e. Analyzing cyberspace vulnerabilities, threats, and incidents that affect the DODIN and providing mitigation/remediation strategies to reduce risk. Supporting the creation, dissemination, and tracking of orders and directives to provide guidance to the DoD community.
- f. Validating compliance of USCYBERCOM orders/directives and facilitating DoD standards/protocols compliance through inspection processes

SECTION C – DESCRIPTION OF WORK

- g. Conducting forensic analysis of compromised information systems and collaborating adversarial activities with the DoD community and partners

Services ISO the Cybersecurity core discipline also include, but are not limited to, contributing to the development of training materials and providing support to the training program for the USCYBERCOM Cybersecurity Workforce Improvement Program (WIP) to ensure an informed, alert, and security-conscious workforce in accordance with DOD 8570.01-M; and reviewing and providing recommendations to appropriate USCYBERCOM personnel for approval to update System Security Plans to aid in the Certification and Accreditation process.

The contractor shall support performance of monthly scans of USCYBERCOM's IT networks to ensure compliance with DOD/National Security Agency (NSA) Information Assurance Vulnerability Alerts (IAVA)/Security Technical Implementation Guides (STIG) and USCYBERCOM 5200-08 requirements.

C.4.8 CORE DISCIPLINE 8 – STRATEGY, POLICY, AND DOCTRINE DEVELOPMENT AND CAMPAIGN ASSESSMENTS

The Strategy, Policy, and Doctrine Development core discipline is defined as contributing to the research, analysis, development, and coordination of Strategy, Policy, and Doctrine for Cyberspace Operations at the national, DoD, U.S. Military Services, and Command level, and national Governmental non-DoD policy level. Additional background information related to this core discipline is provided in Section J (Attachment Q). Services ISO this core discipline include, but are not limited to, reviewing and monitoring incoming Strategies, Policies, Doctrine, orders, plans, Joint Concepts, CONOPs, concepts of employment, and white papers, and analyzing them and making recommendations to ensure correctness and consistency in language, use of doctrinal terms, and impacts to DoD and USCYBERCOM cyberspace strategy, policy, and doctrine objectives.

Additional examples of services ISO this core discipline include, but are not limited to, the following:

- a. Developing white papers, compliance reports and assessment reports in support of activities for defining Strategy, Policy, and Doctrine for authorities
- b. Providing input to the revisions of Strategy, Policy, and Doctrine based on the results of exercises, changes in higher-level guidance, Campaign Assessments, and operational lessons learned
- c. Participating in boards, committees, and working groups with DoD and Inter-Agency partners on matters related to cyberspace Strategy, Policy, and Doctrine.
- d. Supporting the routine assessment of the cyber environment along with the cyber capabilities, tools, and supporting policies for conducting Cyberspace Operations. Tools mandated by the DoD will be provided by USCYBERCOM.
- e. Contributing to the cyberspace policy framework review and revision by examining the current framework using accepted philosophies and models, and validating the applicability of the structure, or repudiating it by recommending more efficient and effective structure, which aligns existing guidance into subordinate DoD, Interagency, and national frameworks

SECTION C – DESCRIPTION OF WORK

- f. Providing technical expertise for Campaign Plan Assessments and conducting analysis. Through this analysis, the contractor shall identify obstacles that might be encountered in achieving military objectives identified in the campaign plan (e.g., sourcing of manpower, policy, authorities). The contractor shall develop plans in order to ensure that MOEs and MOPs are built into the plan in order to leverage during future assessments.

C.4.9 CORE DISCIPLINE 9 – ENGAGEMENT ACTIVITIES

Engagement Activities support is defined as conducting tasks associated with planning, coordinating, and preparing USCYBERCOM for meetings/conferences/visits with Allies, Services, Agencies, Commands, and other parties, to include visit coordination, logistics, and Command information packages. Additional background information related to this core discipline is provided in Section J (Attachment Q).

Services ISO this core discipline include, but are not limited to, the following:

- a. Participating in activities to ensure USCYBERCOM remains in coordination with the USSTRATCOM, and ensure collaboration with other CCMDs, and the Liaison Officers supporting the Lines of Operation (LOO) at various organizations
- b. Providing technical expertise to USCYBERCOM activities with the Joint Staff to capture cyber requirements, cyber training requirements, and to implement and refine interim guidance on the command and control of cyber forces
- c. Providing technical expertise to USCYBERCOM participation in Office of the DoD Chief Information Officer (CIO) engagements for developing policies and with various DoD components and agencies, and for identifying and prioritizing cyber requirements
- d. Planning and coordinating international and domestic partnership engagement activities based on DoD policy guidance and following DoD international agreements and security cooperation processes. This includes maintaining awareness of the policies impacting international and domestic partnership engagements and participating in engagement activities
- e. Collaborating and coordinating with other organizations during capability development efforts to ensure alignment of development with requirements and to avoid duplication of efforts

C.4.10 CORE DISCIPLINE 10 – SECURITY

The Security core discipline is defined as ensuring the Security compliance of organizations, the active promoting of USCYBERCOM Security policies and procedures, and the continual evaluation of the Security integrity of programs. In providing Security support, the contractor shall adhere to USCYBERCOM Security policies and procedures for the safeguarding of classified information.

The Security core discipline encompasses three distinct categories:

- a. Special Security Office (SSO)
- b. Integrated Joint Special Technical Operations (IJSTO)
- c. Alternate Compensatory Control Measures (ACCMs).

SECTION C – DESCRIPTION OF WORK

C.4.10.1 SUB CORE DISCIPLINE 1 - SPECIAL SECURITY OFFICE (SSO) SUPPORT

The SSO ensures that USCYBERCOM affiliates are in compliance with the Security policies outlined in Command Policy Memorandum 2013-01 and all information is safeguarded in accordance with DOD Manual 5200.01 Volumes (1–4) - Information Security Program.

Examples of services in support of the SSO include, but are not limited to, the following:

- a. Providing specialized support, expertise, and products that facilitate the SSO activities and capabilities. The contractor shall have a strong understanding of applicable Federal orders, directives, and guidelines and assist in the review, interpretation, implementation, and application of Security directives, regulations, policies, and procedures.
- b. Providing Security technical expertise for the development of standard operating procedures (SOPs), utilizing the Joint Personnel Adjudication System (JPAS), and scheduling of indoctrination briefings and out-processing of personnel. For example, the contractor shall facilitate the transfer of database records to other databases.
- c. Assisting in monitoring personnel eligibility updates and cross-reference multiple repository databases to prevent unauthorized access to control systems and/or classified information. The contractor shall serve as a responder to messages to the Security Office, and may serve as a point of contact with other Government agencies and departments.
- d. Providing specialized expertise for all Security programs, to include Information Security, Personnel Security, Physical Security, Communications Security, TEMPEST, and Computer Security. For example, the contractor shall develop Security Management documentation (e.g., Security Operating Procedures, CONOPs, and Special Test Plans). For example, the contractor shall conduct Classification Management, Personnel Security (Program Access Request and Personnel File Management), Security Education, and Physical Security (classified destruction, facility inspection) activities.
- e. Ensuring relevant Security guidance is flowed to program management and Security personnel

C.4.10.2 SUB CORE DISCIPLINE 2 - INTEGRATED JOINT SPECIAL TECHNICAL OPERATIONS (IJSTO) / SPECIAL ACCESS PROGRAM (SAP) / ALTERNATE COMPENSATORY CONTROL MEASURES (ACCMS)

The contractor shall provide IJSTO/SAP/ACCM support in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3120.08D, DOD Directive 5205.07, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3213.02C, respectively. CJCSI 3120.08D provides guidelines for the utilization of capabilities within the Special Technical Operations arena. DOD Directive 5205.07. DOD Directive 5205.07

(<http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf>) outlines policy and responsibilities to manage and operate a joint process to ensure the Combatant Commanders and designated members of their staff are afforded knowledge of current and emerging SAP-protected systems, technologies, and methodologies as well as currently available SAP-protected weapon systems and end items appropriate to their missions. Finally, CJCSM 3213.02C provides guidelines for the use of ACCMs to support the Joint Staff Focal Point Program established to ensure need-to-know criteria during the handling of operationally sensitive information.

SECTION C – DESCRIPTION OF WORK

Examples of services required for IJSTO/SAP/ACCM support include, but are not limited to, the following:

- a. Conducting daily maintenance and oversight activities of all IJSTO/SAP Security documents
- b. Providing specialized expertise support pertaining to all facets of the IJSTO administrative/security processes and associated IT and Hardware
- c. Conducting daily management and oversight activities of all IJSTO hardware including accountability and hardware operability assurance
- d. Coordinating with all IJSTO/SAP connectivity providers
- e. Preparing materials and participating in meetings and doctrinal exchanges pertaining to IJSTO, including in-process reviews, command decision briefings, doctrine review committees and doctrine conferences hosted by other services, higher headquarters, and agencies
- f. Providing technical support in development of innovative combat requirements. For example, the contractor shall contribute security inputs to operational planning teams.
- g. Supporting the SAP and ACCM environments
- h. Conducting security read-ins and read-outs and security briefings
- i. Managing administration and documentation of required security training requirements
- j. Collaborating with SAP and other special security managers for maintaining security records

SECTION D - PACKAGING AND MARKING

D.1 PACKAGING AND MARKING

Packaging and marking of all deliverables must conform to normal commercial packing standards to assure safe delivery at destination. Additional requirements may be specified in each Task Order Request (TOR).

D.2 UNCLASSIFIED AND CLASSIFIED MARKING

Unclassified data shall be prepared for shipment in accordance with requirements set forth in the Order, or if none is specified, pursuant to industry standards. Classified reports, data, and documentation shall be prepared for shipment in accordance with requirements set forth in the Order, or if none is specified, pursuant to the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M.

D.3 MARKINGS FOR ELECTRONIC DELIVERY

Electronic copies shall be delivered via email attachment. The contractor shall label each electronic delivery with the Basic Contract and TO Number and Project Title in the subject line of the email transmittal.

Packing, marking and storage costs shall not be billed to the Government unless specifically authorized in the TO.

SECTION E - INSPECTION AND ACCEPTANCE

E.1 ACCEPTANCE FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the FEDSIM Basic Contract CO will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

<https://www.acquisition.gov/far/index.html>

The following clauses apply at the Order level, as applicable, depending upon the contract type of the Order, or as specifically referenced in the applicable Order:

CLAUSE #	CLAUSE TITLE	DATE	FP	COST	TM/LH
52.246-2	INSPECTION OF SUPPLIES—FIXED PRICE	AUG 1996	X		
52.246-2	ALTERNATE I	JUL 1985	X		
52.246-2	ALTERNATE II	JUL 1985	X		
52.246-3	INSPECTION OF SUPPLIES—COST REIMBURSEMENT	MAY 2001		X	
52.246-4	INSPECTION OF SUPPLIES—FIXED PRICE	AUG 1996	X		X
52.246-5	INSPECTION OF SERVICES—COST REIMBURSEMENT	APR 1984		X	
52.246-6	INSPECTION—TIME-AND-MATERIAL AND LABOR-HOUR	MAY 2001			X
52.246-7	INSPECTION OF RESEARCH AND DEVELOPMENT—FIXED PRICE	AUG 1996	X		
52.246-8	INSPECTION OF RESEARCH AND DEVELOPMENT— COST REIMBURSEMENT	MAY 2001		X	
52.246-8	ALTERNATE I	APR 1984		X	
52.246-9	INSPECTION OF RESEARCH AND DEVELOPMENT (SHORT FORM)	APR 1984	X	X	
52.246-11	HIGHER-LEVEL CONTRACT QUALITY REQUIREMENT	FEB 1999	X	X	X
52.246-15	CERTIFICATE OF CONFORMANCE	APR 1984	X	X	X
52.246-16	RESPONSIBILITY FOR SUPPLIES	APR 1984	X		

Quality Assurance

Inspection and quality assurance (QA) activities will be conducted by the Government on all deliverables provided by the contractor under this contract. This includes, but is not limited to, documentation, training, cyber and IT support services and installed IT and COMMS equipment.

SECTION E - INSPECTION AND ACCEPTANCE

Nonconforming Products or Services

Nonconforming products or services will be rejected. The contractor shall maintain as part of the performance record of the contract, records of the following:

1. The number and types of deficiencies found; and
2. Decisions regarding the acceptability of processes, products and corrective action procedures.

Quality Assurance Surveillance Plan (QASP)

The Government will use the attached QASP in Section J (Attachment H) to monitor performance at the individual TO level. The FEDSIM COR will complete QA monitoring forms used to document the inspection and evaluation of the contractor's work performance monthly, at minimum. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

SECTION F – DELIVERABLES OR PERFORMANCE

F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

The following clauses shall apply unless otherwise designated at the Order level. This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the FEDSIM Basic Contract CO will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

<https://www.acquisition.gov/far/index.html>

The following clauses apply at the Order level, as applicable, subject to specific delivery and performance requirements as set forth in the applicable Order.

CLAUSE #	CLAUSE TITLE	DATE	FP	COST	TM/LH
52.211-8	TIME OF DELIVERY	JUN 1997	X	X	X
52.211-8	ALTERNATE I	APR 1984	X	X	X
52.211-8	ALTERNATE II	APR 1984	X	X	X
52.211-8	ALTERNATE III	APR 1984	X	X	X
52.211-9	DESIRED AND REQUIRED TIME OF DELIVERY	JUN 1997	X	X	X
52.211-9	ALTERNATE I	APR 1984	X	X	X
52.211-9	ALTERNATE II	APR 1984	X	X	X
52.211-9	ALTERNATE III	APR 1984	X	X	X
52.211-11	LIQUIDATED DAMAGES – SUPPLIES, SERVICES OR RESEARCH AND DEVELOPMENT	SEP 2000	X		
52.242-15	STOP-WORK ORDER	AUG 1989	X	X	
52.242-15	ALTERNATE I	APR 1984		X	
52.242-17	GOVERNMENT DELAY OF WORK	APR 1984	X		
52.247-34	F.O.B. DESTINATION	NOV 1991	X		
52.247-35	F.O.B. DESTINATION WITH CONSIGNEES PREMISES	APR 1984	X		

F.2 PERIOD OF PERFORMANCE

The ordering period for Basic Contract is a term of five years as follows:

May 20, 2016 through May 19, 2021

The period of performance for each TO awarded under the Basic Contract shall be specified in the TO. Order options, if included at initial issuance of the Order, may be exercised after the expiration date of the Basic Contract. Notwithstanding anything to the contrary above, a multi-year Order placed under the Basic Contract must be consistent with FAR Subpart 17.1 and any applicable funding restrictions.

F.3 PLACE OF PERFORMANCE

The place of performance will be specified in each individual Task Order.

SECTION F – DELIVERABLES OR PERFORMANCE

F.4 DELIVERABLES

The following table contains deliverables required under the Basic Contract. Individual Orders will have additional deliverables specified in each Order. The Government does not waive its right to request deliverables under the Basic Contract, even if such requirements are not specifically listed in this table.

The following abbreviations are used in this schedule:

NLT: No Later Than

TOA: Task Order Award

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall deliver the deliverables listed in the following table:

#	MILESTONE/ DELIVERABLE	REFERENCE & DESCRIPTION	FREQUENCY
1	Public Release of Contract Documents, Redacted Version of Basic Contract	F.5	Within 10 workdays of award of the Basic Contract and each modification
2	Problem Notification Report	F.6	If applicable, the contractor shall provide notice in accordance with Section F.6
3	Contractor Key Personnel Substitution	G.2 If a substitution occurs, provide notification	Within 5 calendar days of the substitution
4	Subcontracting Reports	Section J, Attachment P	Within 30 calendar days after the close of each annual reporting period
5	Mergers, Acquisitions, Novations, and Change-of-Name Agreements	G.4.1	Copy of SF 30 and other applicable documents within 45 calendar days of finalization
6	Forward Pricing Rate Agreements (FPRA), Forward Pricing Rate Recommendations (FPRR) and/or Approved Billing Rates	G.4.2 If applicable, correspondence and audit reports from DCAA/Defense Contract Management Agency (DCMA) or other cognizant auditing entity that updates the current status	Within 30 calendar days after the update

SECTION F – DELIVERABLES OR PERFORMANCE

#	MILESTONE/ DELIVERABLE	REFERENCE & DESCRIPTION	FREQUENCY
7	Cost Accounting Standards (CAS)	H.7 If applicable, correspondence and audit reports from DCAA/DCMA that updates the current CAS Disclosure Statements, Administration of CAS, or Cost Accounting Practice Changes	Within 15 calendar days after the update
8	Approved Purchasing System	H.8 If applicable, correspondence and audit reports from DCMA or other cognizant auditing entity that updates the current status	Within 15 calendar days after the update

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14. The contractor shall deliver the deliverables to the CO and COR listed in Section G.

F.5 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the Basic Contract, or any modification to the Basic Contract (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of the General Services Administration (GSA). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

SECTION F – DELIVERABLES OR PERFORMANCE

F.6 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media, as well as placing in USCYBERCOM's designated repository. The following are the required electronic formats, whose versions must be compatible with Microsoft Office versions utilized by USCYBERCOM.

Text	MS Word
Spreadsheets	MS Excel
Briefings	MS PowerPoint
Drawings	MS PowerPoint (preferred), MS Visio,
Schedules	MS Excel (preferred), MS Project

F.7 PLACE(S) OF DELIVERY

At the Basic Contract level, deliverables shall be delivered to the FEDSIM Basic Contract CO and FEDSIM COR listed in Section G.1.1.

At the individual TO level, unclassified deliverables and correspondence shall be delivered to the COR and USCYBERCOM Technical Point of Contact (TPOC) specified in individual TOs. Classified deliverables shall be delivered to the USCYBERCOM TPOC and notice of the delivery shall be provided to the Ordering CO and FEDSIM COR.

F.8 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR and copy the TPOC via a Problem Notification Report (PNR) provided in Section J (Attachment C) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

SECTION G – CONTRACT ADMINISTRATION DATA

G.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR)

The FEDSIM Basic Contract CO will appoint a FEDSIM Basic Contract COR in writing for the Basic Contract using a COR Appointment Letter in Section J (Attachment A). The FEDSIM Basic Contract COR will provide no supervisory or instructional assistance to contractor personnel.

At the order level, the CO awarding each order under this Basic Contract (referred to as the Order or Ordering CO), may appoint a COR (referred to as the Order or Ordering COR) in writing for that order through a COR Appointment Letter that will be provided to the contractor upon award of the order (the OCO may use the format in Section J (Attachment A), or another format specified in the Order RFQ). The COR will receive, for the Government, all work called for by the Order and will represent the Ordering CO in the technical phases of the work. The Ordering COR will provide no supervisory or instructional assistance to contractor personnel.

The Basic Contract or Ordering CORs are not authorized to change any of the terms and conditions, scope, schedule, and price of the Basic Contract or the order. Changes in the scope of work will be made only by the Ordering CO by properly executed modifications to the Order, or by the FEDSIM Basic Contract CO, by modification to the Basic Contract.

G.1.1 CONTRACT ADMINISTRATION

For the Basic Contract, the following FEDSIM CO is responsible for contract administration

Contracting Officer:

Robert Wade
GSA FAS AAS FEDSIM
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (202) 603-0283.
Email: robert.wade@gsa.gov

Contracting Officer’s Representative:

Ibrahim Kent
GSA FAS AAS FEDSIM
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405
Telephone: (215)528-2910
Email: Ibrahim.kent@gsa.gov

Technical Point of Contact:

Tiffany B Traynor
Chief, Contracts Management Branch
USCYBERCOM J831
Telephone: (240)373-9028
Email: tbtrayn@cybercom.

SECTION G – CONTRACT ADMINISTRATION DATA

G.2 ROLES AND RESPONSIBILITIES OF BASIC CONTRACT CONTRACTOR KEY PERSONNEL

The contractor shall assign a Corporate IDIQ Program Manager and Corporate IDIQ Contracts Manager to represent the contractor as primary points of contact to resolve issues, perform Basic Contract level duties, and other functions that may arise relating to the Basic Contract and TOs solicited and awarded under the Basic Contract. If the offeror proposes additional Key Personnel at the Basic Contract level, the offeror shall provide rationale for including additional Key Personnel. Additional Key Personnel requirements may be designated by the Ordering CO at the TO level.

There is no minimum qualification requirements established for contractor Key Personnel. Additionally, contractor Key Personnel at the Basic Contract level do not have to be full-time positions; however, the contractor Key Personnel are expected to be fully proficient in the performance of their duties.

The contractor shall ensure that the FEDSIM Basic Contract CO has current point-of-contact information for both the Corporate IDIQ Program Manager and Corporate IDIQ Contracts Manager. In the event of a change to contractor Key Personnel, the contractor shall notify the FEDSIM Basic Contract CO and provide all point-of-contact information for the new Key Personnel within five calendar days of the change.

All costs associated with contractor Key Personnel duties shall be handled in accordance with the contractor's standard accounting practices; however, no costs for contractor Key Personnel may be billed to the Basic Contract.

Failure of contractor Key Personnel to effectively and efficiently perform their duties will be construed as conduct detrimental to contract performance and may result in activation of Dormant Status and/or Off-Ramping.

G.2.1 CORPORATE IDIQ PROGRAM MANAGER

The contractor's corporate management structure shall provide senior, high-level, program management of the Basic Contract Program, including a Corporate IDIQ Program Manager to represent the company in all Basic Contract program-related matters.

The Corporate IDIQ Program Manager duties include, but are not limited to:

- a. Being ultimately responsible for ensuring that all reporting information required under the Basic Contract is provided accurately, thoroughly, and timely
- b. Being ultimately responsible for all performance issues related to the Basic Contract and TOs awarded under the Basic Contract
- c. Attending all IDIQ Program Management Review (PMR) Meetings and other Basic Contract meetings as scheduled

G.2.2 CORPORATE IDIQ CONTRACTS MANAGER

The contractor's corporate management structure shall provide senior, high-level, program management of the Basic Contract Program, including a Corporate Contracts Manager to represent the company in all Basic Contract related matters.

The Corporate Contracts Manager duties include, but are not limited to:

SECTION G – CONTRACT ADMINISTRATION DATA

- a. Ensuring the company's TO awards under the Basic Contract are contractually in compliance with the Basic Contract
- b. Ensuring contract administrative functions and meeting all the performance reporting and compliance standards listed under Section F are maintained
- c. Being ultimately responsible for ensuring that all contractual agreements, including modifications, are negotiated and put in place expeditiously
- d. Being ultimately responsible for ensuring that all TO invoicing is accurate and timely
- e. Attending all Basic Contract PMR Meetings and other Basic Contract meetings as scheduled.

G.3 INVOICE REQUIREMENTS

Invoices shall be submitted at the TO level, and not the Basic Contract level.

G.4 CONTRACTOR ADMINISTRATION REQUIREMENTS

G.4.1 MERGERS, ACQUISITIONS, NOVATIONS, AND CHANGE-OF-NAME AGREEMENTS

If a contractor merges, is acquired, or recognizes a successor in interest to Government contracts when contractor assets are transferred; or recognizes a change in a contractor's name; or executes novation agreements and change-of-name agreements by a CO other than the FEDSIM Basic Contract CO, the contractor must notify the FEDSIM Basic Contract CO and provide a copy of the novation or any other agreement that changes the status of the contractor.

G.4.2 FORWARD PRICING RATE AGREEMENTS, FORWARD PRICING RATE RECOMMENDATIONS, AND APPROVED BILLING RATES

Billing rates and final indirect cost rates may be used in reimbursing indirect costs under cost-reimbursement TOs and in determining progress payments under fixed-price TOs.

A DCAA-approved Forward Pricing Rate Agreement (FPRA) means a written agreement to make certain rates available during a specified period for use in pricing contracts or modifications. These rates represent reasonable projections of specific costs that are not easily estimated for, identified with, or generated by a specific contract, contract end item, or task. These projections may include rates for such things as direct labor, indirect costs, material obsolescence and usage, and material handling.

A Forward Pricing Rate Recommendation (FPRR) means a set of rates and factors unilaterally established by the DCMA Administrative Contracting Officer (ACO) for use by the Government in negotiations or other contract actions when forward pricing rate agreement negotiations have not been completed or when the contractor will not agree to a forward pricing rate agreement.

Approved Billing Rates means an indirect cost rate established temporarily for interim reimbursement of incurred indirect costs and adjusted as necessary pending establishment of final indirect cost rates.

For T&M, LH, and Cost-Reimbursement (all types) TOs solicited and awarded under the Basic Contract, contractors are encouraged to execute a FPRA and/or approved billing rates to the

SECTION G – CONTRACT ADMINISTRATION DATA

maximum extent practicable. Contractors may use FPRRs when an FPRA has not been negotiated.

The contractor shall notify the FEDSIM Basic Contract CO and designated Ordering CO for affected TOs, in writing (see Section F.4), if there are any changes in the status of its FPRA, FPRR, and/or approved billing rates and provide the reasons for the change and copies of audit reports, as applicable.

G.5 BASIC CONTRACT TASK ORDER PROCESS

In accordance with Section B.1, TOs will be used to order services. All TOs will be issued in accordance with the fair opportunity procedures of 48 C.F.R. 16.505(b) and DFARS 216.505. The minimum guarantee of the Basic Contract is \$2,500.00, as identified in Section B.1.2. One or more TOs may be issued during the performance period of the Basic Contract; it is understood and agreed that the Government has no obligation to issue any more than one TO. COs of the GSA/Federal Acquisition Service (FAS) are authorized ordering officers. Services to be furnished under this contract shall be furnished at such times as ordered by the issuance of the TO by the CO. All Orders are subject to the terms and conditions of this contract. This contract shall control in the event of conflict with any TO.

G.5.1 TASK ORDER REQUEST (TOR)

A TOR will be used to solicit TO proposals under this contract. The TOR may include specific metrics and quality assurance methods (if applicable). The TOR may also include provisions for incentive fee, award fee, or fixed fee.

Unless an exception to fair opportunity applies, all Basic Contract holders will receive each TOR issued by a GSA CO.

All TORs will incorporate all terms and conditions of the Basic Contract. In addition, the TOR will normally include the following to the extent applicable to individual TOs:

- a. A Statement of Objectives (SOO), Statement of Work (SOW), or Performance Work Statement (PWS) describing the work to be performed, the deliverables, the period of performance, Government point(s) of contact, description of marking information, data rights, inspection and acceptance of services, security requirements, and Government-Furnished Information (GFI) / Property (GFP), as applicable
- b. The submission date/time and the method of delivery for proposals
- c. Specific instructions on what to include in the proposal submission. This may include oral presentations and written responses summarizing technical and price approaches.
- d. Evaluation factors and their relative order of importance
- e. Other information deemed appropriate by the Ordering CO

G.5.2 TASK ORDER PROPOSAL SUBMISSION

Basic Contract awardees shall be capable of providing a proposal within two workdays for urgent requirements. For non-urgent requirements, the Basic Contract awardees shall submit proposals within 30 calendar days of issuance of the TOR, unless otherwise specified in individual TOs. At a minimum, the proposal shall include:

SECTION G – CONTRACT ADMINISTRATION DATA

- a. The proposal may include a detailed cost breakout of all labor required to accomplish the tasks as set forth in the TOR or be a fixed-price proposal with sufficient information to substantiate the price proposed
- b. Organizational Conflict of Interest Statement disclosing any known or expected conflicts of interest pursuant to FAR 9.5
- c. The proposal may also require the submission of the following information (the Government is not limited to the below list and may require other information):
 1. Technical information, e.g., technical approach, including subcontractors and experience as required by the TOR.
 2. Corporate Experience or Past Performance
 3. Proposed Key Personnel
 4. Proposed PWS (if a SOO is issued)
 5. Other information deemed appropriate by the Ordering CO.

G.5.3 TASK ORDER EVALUATION

The Government will evaluate responses against evaluation criteria contained in the proposed TOR. The Government's award decision will be based on best value to the Government, price and other factors considered, unless otherwise specified in the TOR.

G.5.4 TASK ORDER ISSUANCE

A TO is considered issued when it is signed by the GSA CO and transmitted to the contractor. Transmittal is complete when the awardee receives a notification of award from GSA's ASSIST system. A GSA Federal Acquisition Service (FAS) CO shall act as the TO CO and is responsible for issuing any TOs placed hereunder. The SOW / PWS, labor mix and hours (if applicable), and proposed costs / price for the TOR may be incorporated into any resulting TO. The proposed technical solution may also be incorporated in the TO. At any time during the duration of the Basic Contract, the FEDSIM Basic Contract CO reserves the right to revise the procedures pertaining to TO issuance. Ordering COs may only issue a TO with written approval from the FEDSIM Basic Contract CO. COs from GSA FAS are the only individuals that are authorized to issue TOs and obligate the Government for TOs awarded under the Basic Contract. TOs and modifications shall be made in writing and be signed by any authorized GSA FAS CO. Each TO shall, as appropriate:

- a. Set forth a pricing schedule
- b. Set forth the specific level of effort and/or performance outcomes desired to be fulfilled under the TO based on the estimated dollar value and complexity of the Government's requirement
- c. Designate the TO COR and TPOC who will perform inspection and acceptance
- d. Set forth any payment provisions (e.g., progress payments, milestone billings)
- e. Be dated

SECTION G – CONTRACT ADMINISTRATION DATA

- f. Set forth the property, if any, to be furnished by the Government and the date(s) such property is to be delivered to the contractor
- g. Set forth the disbursing office where payment is to be made
- h. Set forth administration data (e.g. invoicing instructions)
- i. Set forth the Government's technical data rights
- j. Set forth any other pertinent information

Unauthorized Work: The contractor is not authorized to commence TO performance prior to CO notice to proceed.

Ordering Period: The Ordering Period shall be commensurate with the period of the Basic Contract. Accordingly, TOs for services specified in the PWS of the Basic Contract may be issued by any CO from GSA FAS until the final day of the Basic Contract. TO periods of performance shall not be longer than five years total.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.1 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel at the individual TO level without the written concurrence of the Ordering CO. Prior to utilizing other than personnel specified in proposals in response to the TOR, the contractor shall notify the Ordering CO and the COR of the existing TO. This notification shall be no later than 5 calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance, unless otherwise approved by the FEDSIM COR.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by Federal Acquisition Regulation (FAR) 52.249-6 Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

Substitutions of key personnel associated with prolonged leave (leave in excess of two weeks for reasons of training, vacation, etc.) shall occur only after the Government has received notice. Substitutes shall have qualifications equal to or higher than the qualifications of the individual to be replaced. Notification of any key personnel substitution from the contractor to the government shall include the following information:

- a. Explanation of the circumstances necessitating the substitution
- b. Duration of the substitution
- c. Complete resume of the proposed substitute
- d. Other information requested by the CO to support an assessment of relative qualification of the proposed substitute

H.2 GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide workspace, computers, connectivity, and other resources required to accomplish the tasks outlined in Section C and as specified in individual TOs for those contractor employees located at Government facilities. Contractors located at offsite facilities may receive Government-Furnished Equipment (GFE) to perform the tasks defined in Section C. Individual TOs will designate whether offsite contractor employees will receive GFE.

The Government will provide access to non-procurement-sensitive documentation, information on various weapon systems, program process and schedules, as well as intelligence and information pertaining to cyberspace activities in support of military information operations, related activities, and associated follow-on tasks to enable contractors to complete their assigned tasks.

Information will include reports, briefings, and other related reference material. The Government will provide the contractor with timely information, to include access to both unclassified and classified Government information networks, and will facilitate contractor personnel interfaces with other DoD staff, service staff, and national agency offices as required to complete this effort.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.3 SECURITY REQUIREMENTS

H.3.1 GENERAL SECURITY REQUIREMENTS

All TOs issued under this contract will be in support of classified programs. In order to be eligible to provide support to classified programs, prime contractors (to include team members and subcontractors) shall be either a U.S.-owned firm or possess a favorable National Interest Determination if foreign owned. The prime contractor, its subcontractors, and its teaming partners must have a final TS Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB) at time of proposal submission.

The contractor must have readily available access to Defense Security Services (DSS)-certified work locations for performing classified work up to and including TS/Sensitive Compartmented Information (SCI) at time of contract award. Individuals performing work under resultant tasks orders must be a U.S. citizen and comply with applicable program security requirements. All contractors performing under resulting TOs shall possess a TS personnel security clearance with SCI access eligibility and a Counterintelligence (CI) polygraph at time of proposal submission for those personnel identified by name in the proposal and time of project start for all other personnel. The contractor shall comply with all appropriate security regulations in handling classified material and in publishing reports and other products. See also attached DD-254 in Section J (Attachment I).

H.3.2 SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF)

The contractor shall have readily available access to DSS-certified work locations for performing classified work up to and including TS/SCI at time of contract award. The contractor must comply with DOD 5220.22M National Industrial Security Program Manual (NISPOM) and have access to a SCIF. The SCIF access may or may not be within 50 miles of Fort George G. Meade, Maryland. SCIF access may be through a team member.

H.3.3 PERSONNEL SECURITY REQUIREMENTS

All contractors shall possess a final TS clearance with SCI eligibility. All contractors shall have been granted full SCI eligibility by a U.S. Government Adjudication Authority within the past 60 months and have not had a break in SCI access of more than 24 months during this period. All contractors shall also have a Counterintelligence Scope Polygraph (CSP) examination conducted by a recognized U.S. Government polygraph entity within seven years (in scope) and meet Personnel Security Standards and Procedures Governing Eligibility for Access to SCI. The contractor shall have successfully undergone a Single Scope Background Investigation (SSBI) that is current (in scope) as defined by DOD 5200.2-R, DODM 5105.21-V3, and ICD 704 prior to being assigned to this contract. The nature of the contract requires contractor personnel to possess a high degree of security awareness. All contractors must receive security indoctrination by USCYBERCOM and must be vetted and approved for access by the National Security Agency (NSA) Military Affairs Desk Office (MADO) prior to access to USCYBERCOM classified information, spaces, and IT systems and networks being granted. Contractors may be required to sign a USCYBERCOM Non-Disclosure Agreement (NDA) based on the tasks to be performed.

The contractor shall maintain a database of personnel with active security clearances and initiate periodic background updates as required. All contractors working on this contract must submit

SECTION H – SPECIAL CONTRACT REQUIREMENTS

to, obtain, and successfully complete a CSP examination should their current polygraph expire during performance. Any unfavorable information developed during any investigation or other official inquiry shall result in removal from this contract in accordance with established procedures. Contractor personnel shall keep the USCYBERCOM SSO Division and the COR apprised of any significant security concerns and/or changes in personal status that could affect their eligibility for access to SCI to include:

- a. Any travel to a foreign country and/or proposed visits to foreign embassies. Personnel must report all foreign travel, official and unofficial, in advance of the travel and agree to forego personal unofficial foreign travel when it is deemed by agency approving authorities to constitute a hazard to national security.
- b. Close and/or continuing contact with citizens of a foreign country. Any unusual or suspicious contacts or incidents with foreign nationals.
- c. Any arrest or court actions other than minor traffic violations (over \$300)
- d. Any change in marital status or cohabitation. If, following employment, an employee marries (or cohabits with) a foreign national, termination of employment may be affected.
- e. Any significant financial issues (including, but not limited to, unexplained affluence, bankruptcy, judgment, garnishment, lien, or other significant financial difficulties)
- f. Any unauthorized computer network activities
- g. Any issues or concerns regarding classified or sensitive information (inadvertent, unauthorized or improper carrying or removal of classified material; any attempts by unauthorized persons to obtain classified information; or divulgence of classified information to media representatives or in an otherwise public forum)
- h. Any current or changes in mental health condition (minus sexual assault victimization) that would cause an objective observer to have a concern about your judgment, reliability, or trustworthiness in relation to your work
- i. Any other activity that could negatively affect or influence the impact the security of USCYBERCOM, its personnel, installations, information, and/or activities

In accordance with DOD 5200.2-R, Section C2.1, all individuals shall be U.S. citizens. All contractor personnel working on or managing this effort shall strictly adhere to USCYBERCOM and NSA security regulations and procedures. All members of the contractor team (prime, sub-contractors, etc.) providing personnel, including supervisory personnel to perform the work, must comply with the applicable clearance levels (facilities/personnel) based on the sensitivity of the task/work requiring a clearance. The COR must keep and maintain a current and accurate list of all contract affiliates performing on specific contracts. With the exception of approved courier duties, contractor personnel shall not remove classified information from the worksite, either physically or electronically, and under no circumstances shall the contractor or its personnel allow any classified information be stored at an off-site facility. Contractor personnel shall ensure continuing adherence to accepted Government IT policies and guidance applicable to this RFP. This includes public laws, executive orders, directives, regulations, manuals, standards, memorandums, and instructions.

Contractor personnel shall fully comply with USCYBERCOM and NSA in-processing and out-processing guidelines. At a minimum, the contractor shall:

SECTION H – SPECIAL CONTRACT REQUIREMENTS

- a. Be indoctrinated by USCYBERCOM Security and NSA Security and sign USCYBERCOM and NSA NDAs
- b. Follow the Agency's support agreement and shall be required to prepare/submit IT-related work orders and ensure work orders are executed
- c. Notify the COR of the employee's departure and his/her successful out-processing on the last day of work. At a minimum, successful out-processing shall require the turn-in/collection of all: (1) security badges; (2) Smart cards and/or other comparable security devices; and (3) GFE issued to employee for performance of duties in accordance with local procedures. Successful out-processing also requires the employee receive a security debrief.
- d. Aggressively collect/recover and turn in security badges and devices, smart cards, and GFE to the COR or designee in the event the contractor employee fails to successfully out-process. Every effort shall be made to ensure these are recovered/ turned in within 24 hours (one business day) of the departing employee's last day of work.
- e. Coordinate changes in employment status with the COR affecting the accuracy of security badges and supporting records within 24 hours (one business day) of any such changes to ensure the appropriate devices are promptly reissued and/or collected
- f. Account for, protect, and return Government-issued badges, identification cards, passes, vehicle registration media, and admittance controls that are U.S. Government property to the Government at the end of the contract period of performance or at any other time as required. When a contractor employee leaves the company, or ceases working on this contract, the employee shall adhere to all required USCYBERCOM out-processing procedures.
- g. Not bill the Government for contractor personnel pending successful indoctrination by both USCYBERCOM and NSA security officials unless working directly on the contract and providing contract deliverables, or as approved by the COR. Should contractor personnel be denied access to the host agency facilities and classified networks for any reason, that individual shall not be counted towards the contractor's required staffing level.

H.4 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.4.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

- a. If an offeror is currently providing support, or anticipates providing support that creates or represents an actual or potential organizational conflict of interest (OCI), the offeror shall immediately disclose this actual or potential OCI to GSA in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
- b. The Contractor is required to complete and sign an OCI statement per Section L.5.1 of this RFP. The offeror must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, proving all current information bearing on the

SECTION H – SPECIAL CONTRACT REQUIREMENTS

existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below and Section L.5.1 of the RFP.

- c. If an offeror with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review.
- d. In addition to the mitigation plan, the CO may require further relevant information from the offeror. The CO will use all information submitted by the offeror, and any other relevant information known to GSA, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
- e. If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government and the offeror may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid neutralize, mitigate, or waive such conflict in the contract awarded.

H.5 NON-DISCLOSURE AGREEMENT

The contractor shall recognize that in the performance of this contract it may receive or have access to certain sensitive information, including information provided on a proprietary basis by other contractors, equipment manufacturers, and other private or public entities. The contractor agrees to use and examine this information exclusively in the performance of this contract, and to take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government or Government-designated support contractors possessing appropriate proprietary agreements, as listed in the subsections below.

H.5.1 INDOCTRINATION OF PERSONNEL

The contractor agrees to indoctrinate its personnel who have access as to the sensitive nature of the information and the relationship under which the contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture, or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The NDA for Contractor Employees provided in Section J (Attachment R) shall be signed by all indoctrinated personnel and forwarded to the COR for retention prior to work commencing. The contractor shall restrict access to sensitive/proprietary information to the minimum number of employees necessary for contract performance.

H.5.2 SIGNED AGREEMENTS

- a. The contractor further agrees to sign an agreement to this effect with carriers and other private or public entities providing proprietary data for performance under this contract. As part of this agreement, the contractor shall inform all parties of its agreement to allow certain Government-designated contractor's access to all data as described in paragraph (c) below. One copy of each signed agreement shall be forwarded to the CO. These shall be signed prior to work commencing.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

- b. In addition, the contractor shall be required to coordinate and exchange directly with other contractors as designated by the Government for information pertinent and essential to performance of TOs issued under this contract. The contractor shall discuss and attempt to resolve any problems between the contractor and those contractors designated by the Government. The CO shall be notified in writing of any disagreement(s) which has (have) not been resolved in a timely manner, and shall furnish the CO copies of communications between the contractor and associate contractor(s) relative to contract performance. Further, the close interchange with or between contractor(s) may require access to or release of proprietary data. In such an event, the contractor shall enter into agreement(s) with the Government-designated contractor(s) to adequately protect such proprietary data from unauthorized use or disclosure so long as it remains proprietary. A copy of such agreement shall be provided to the CO.
- c. Government-Designated Contractors. The contractor agrees to allow the below listed Government-designated support contractors, possessing appropriate USCYBERCOM and NSA NDAs and retained by the Government to advise the Government on cost, schedule, and technical matters pertaining to this acquisition, access to any unlimited rights data (as defined in DFARS 252.227-7013) acquired under the terms and conditions of this contract and to sign reciprocal USCYBERCOM and NSA NDAs with them. One copy of each signed agreement shall be forwarded to the CO.

List of designated contractors: *Provided at the individual TO level.*

- d. All Government-designated contractors stated herein, or added at a future date, shall also enter into USCYBERCOM and NSA NDAs with all parties providing proprietary information to the contractor, and the USCYBERCOM and NSA NDAs shall be signed before work commences.
- e. Remedy for Breach. The contractor agrees that any breach or violation of the certifications or restrictions of this clause shall constitute a material and substantial breach of the terms, conditions, and provisions of the contract and that the Government may, in addition to any other remedy available, terminate this contract for default in accordance with the provisions of FAR 52.249-6. Nothing in this clause or contract shall be construed to mean that the Government shall be liable to the owners of proprietary information in any way for the unauthorized release or use of proprietary information by this contractor or its subcontractors.

H.6 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed at the order level shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact

SECTION H – SPECIAL CONTRACT REQUIREMENTS

web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.7 COST ACCOUNTING SYSTEM

The contractor is required to have an acceptable cost accounting system for Cost Reimbursement type Orders in accordance with DFARS 252.242-7006. The contractor must maintain a cost accounting system determined adequate by its cognizant auditing agency. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract.

The contractor shall notify the ACO and designated Ordering COs for ongoing Orders, in writing, if there are any changes in the status of its cost accounting system and provide the reason(s) for the change.

H.8 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. The contractor is required to have an acceptable purchasing system in accordance with DFARS 252.244-7001.

Advance notification requirements for subcontracting and consent to subcontract are not required, unless otherwise requested by the Ordering CO, when a Contractor has an approved purchasing system on an individual task order or task orders with no subcontracting possibilities or for commercial items acquired under FAR Part 12.

An Approved Purchasing System is not mandatory; however, Contractors are encouraged to have a purchasing system approved by the Defense Contract Management Agency (DCMA) or other cognizant Government administration office for the entire term of the Basic Contract.

Prior to the award of a TO, the CO shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of its purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within ten workdays from the date the results are known to the contractor.

H.9 EARNED VALUE MANAGEMENT (EVM)

When EVM is determined to be applicable to an individual TO, the contractor shall employ EVM in the management of the individual TOs in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, *Earned Value Management Systems*. A copy of the standard is available at <http://global.ihs.com/>. The Government expects the contractor to employ innovation in its proposed application of EVM techniques to this TO in accordance with best industry practices.

H.10 SUBCONTRACTOR LISTS

Prime contractors (Primes) shall provide a list of all subcontractors (team members) with their initial proposal at the individual TO level. Any time a prime desires to add or delete a subcontractor, the prime contractor shall provide an updated list to the Contracting Officer for

SECTION H – SPECIAL CONTRACT REQUIREMENTS

review and approval. Primes are encouraged to foster long-term relations with subs on their teams. The prime contractor is responsible for providing timely notification to the Government of any acquisition or mergers involving the prime contractor to include the potential impact on this contract.

The Government may request procedures as referenced in FAR 42.12, Novation and Change-of-Name Agreements, be implemented and may suspend a prime contractor team or individual subcontractor from the contract team until all contract administration procedures are completed.

H.11 TRAVEL

H.11.1 TRAVEL REGULATIONS

Only long-distance travel will be reimbursed at the TO level. Long-distance travel is defined as over 50 miles from the place of performance of the individual TO, unless otherwise specified. Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous US
- b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the US
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.11.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the Federal Systems Integration and Management Center (FEDSIM) COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, or DSSR.

Requests for travel approval shall include, at minimum:

- a. Be prepared in a legible manner
- b. Include a description of the travel proposed including a statement as to purpose
- c. Be summarized by traveler
- d. Identify the TO number
- e. Identify the CLIN associated with the travel
- f. Name of the Government point of contact who requested the travel
- g. Be submitted in advance of the travel with sufficient time to permit review and approval

SECTION H – SPECIAL CONTRACT REQUIREMENTS

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.12 TOOLS (HARDWARE/SOFTWARE) AND/OR ODCs

Tools and ODCs are defined as follows:

- a. Tools - Hardware and/or software critical and related to the services being acquired under the contract
- b. ODCs - Ancillary supplies critical and related to the services being acquired under the contract

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under individuals TOs. Such requirements will be identified at the time a TOR is issued or may be identified during the course of the individual TO by the Government or the contractor. If the contractor initiates a purchase within the scope of the TO and the prime contractor has an approved/acceptable purchasing system, the contractor shall submit to the COR a Request to Initiate Purchase (RIP). If the prime contractor does not have an approved/acceptable purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO and without complying with the requirements of Commercial Software Agreements at the individual TO level.

H.13 DATA AND PROPERTY RIGHTS

H.13.1 GOVERNMENT-FURNISHED DATA AND MATERIALS

The Government shall retain all rights and privileges, including those of patent and copy, to all Government-furnished data. The contractor shall neither retain nor reproduce for private or commercial use any information or other materials furnished or made available under this contract (to include all TOs). The contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are in addition to any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract or any TO.

H.13.2 CONTRACTOR PRODUCED DATA AND MATERIALS

All property rights, including publication rights, in the information and materials first produced by the contractor in connection with this contract (to include all TOs) shall vest in the Government. Information and materials shall include, but are not limited to, computer software applications/databases, software documentation, plans, systems analysis, reports, extracts, test data, and procedures.

H.13.3 COMMERCIAL COMPUTER SOFTWARE

At a minimum, the rights of the Government regarding the use, reproduction, and disclosure of commercial computer software provided under a TO shall be as described in Section I, DFARS clause 252.227-7013. Additional rights may be specified by the Government in a TOR.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

H.14 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in DFARS, 252.227-7013, 252.227-7014, 252.227-7015 and/or FAR 52.227-13 shall apply when applicable. The Software Agreements, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools and shall prevail over any inconsistent provision in DFARS 252.227-7015 to the extent of such inconsistency.

H.15 INTERNATIONAL TRAFFIC AND ARMS AGREEMENT (ITAR) REGULATIONS

The requirements of this Basic Contract require presenting, discussing, and engaging in technical discussions (defense services) involving ITAR controlled technical data with the Government Defense Agencies. In order for the contractor (to include subcontractors, consultants, and teaming partners) to engage in technical discussions (defense services) with a Foreign Person, it shall be ITAR compliant with either a Technical Assistance Agreement (TAA) or an ITAR Exemption authorizing export privileges with the cooperative partners. ITAR compliance means being registered with the U.S. Department of State (DoS) and having the proper ITAR authorizations to conduct defense services. In order to submit a request for ITAR authorization, the U.S. applicant (to include all subcontractors, consultants, and teaming partners) must be registered with the Directorate of Defense Trade Controls (DDTC) and DoS and the registration has to be current (renewable each year).

H.16 PROHIBITION AGAINST SOLICITING AND PERFORMING PERSONAL SERVICES

- a. The performance of personal services under this contract is strictly prohibited. Personal service contracting is described in FAR Subpart 37.104. A number of factors considered individually or collectively, may constitute personal services. Each contract must be judged in consideration of the particular facts and circumstances, but the question relative to personal services is: Will the Government exercise relatively continuous supervision and control over the contractor personnel performing the contract?
- b. The Government and contractor understand and agree that support services to be provided under this contract are non-personal services in nature. That is, no employer-employee relationship exists or will exist between the Government and the contractor or between the Government and the contractor's employees.
- c. To this end, contractor personnel under this contract shall not:
 - i. Be placed in a position where they are appointed or employed by a Federal employee or are under the supervision, direction, or evaluation of a Federal employee
 - ii. Be placed in a Federal staff or policy making position
 - iii. Be placed in a position to supervise, direct or evaluate Federal employees, personnel of other contractors or otherwise be a part of the Government

SECTION H – SPECIAL CONTRACT REQUIREMENTS

- d. The contractor shall appoint a supervisor/manager that will be the contractor's authorized representative for technical and administrative performances of all services required in relation to the contract/TO. The supervisor shall serve as the single point of contact through which all substantive contractor/Government communications, work, and technical direction flow.
- e. Rules, regulations, direction, and requirements relative to good order, administration and security are applicable to all individuals that enter a Government installation. In no manner shall it be construed or interpreted that the existence of a Government installation-type environment is contrary to the mutually agreed non-personal services nature of contract performance.
- f. The contractor shall immediately notify the CO in the event the contractor or its employees are directed by any Government employee to perform work which the contractor considers to be personal services.

H.17 SECURITY INVESTIGATIONS AND REPLACEMENT PERSONNEL

- a. Security investigations are very costly to the Government. The contractor shall make every effort to preclude incurrence of costs by the Government for security investigations during initial on-boarding and in relation to replacement personnel by providing professionally qualified, personally reliable, physically able employees of reputable background, possessing sound character, and available for a minimum employment period no less than one year in each case.
- b. Government-initiated security investigations do not relieve the contractor of its responsibility to provide employees suitable for security investigation purposes.
- c. In the event a security investigation conducted by the Government of a contractor-furnished employee results in an ineligible security determination or a contractor-furnished employee needs to be replaced due to performance or security matters, the instance will be evaluated by the Government for the purpose of establishing whether or not the contractor abdicated its responsibility to select suitable employees, i.e., professionally qualified, personally reliable, physically able employees of reputable background, possessing sound character and available for employment for a period no less than one year in each case.
- d. When a contractor fails to comply with the terms of this clause, the contractor may be held monetarily responsible to include reasonable and necessary costs incurred by the Government to:
 - i. Provide coverage/performance throughout the minimum employment period in cases where the absence of contractor personnel would cause a security threat or program disruption
 - ii. Conduct security investigations in excess of those otherwise required
- e. Nothing in this clause shall require the contractor to bear costs associated with security investigations concerning replacement personnel in the case(s) of serious illness/condition or death.

SECTION H – SPECIAL CONTRACT REQUIREMENTS

- f. The contractor must provide notice to the Government before any Government-initiated security investigation and prior to offering any employee for contract/TO performance when the employee is expected to perform less than the minimum employment period of one year for any reason. At the discretion of the Government, in exceptional cases subject to prior Government approval, a minimum employment period less than one year may be authorized.
- g. Consideration/reimbursement of any kind to which the Government may be entitled pursuant to this clause does not restrict or otherwise limit the full force and effect of rights and remedies otherwise available to the Government in the contract or otherwise established by law.

H.18 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.19 SMALL BUSINESS SUBCONTRACTING GOALS

For any subcontracted dollars under the contract, the Government has incorporated the following small business goals:

- a. 50 percent – Total Small businesses including HUBZone, SDB, WOSB and SDVOSB

Furthermore of the 50 percent goal for Small Business, the following also should apply

- b. 2 percent – HUBZone small businesses
- c. 15 percent – Small Disadvantaged Businesses (SDB)
- d. 9 percent – Women-Owned Small Businesses (WOSB)
- e. 7 percent – Service Disabled Veteran-Owned Small Businesses (SDVOSB)

For Example:

Categories	Sample Dollars	Percentages
Total Dollars to be subcontracted	\$ 25,000,000	100%
To: Large Business	\$ 12,500,000	50%
To all: Small Business (includes sub-categories	\$ 12,500,000	50%
HUBZone Small Business	\$ 500,000	2%
Small Disadvantaged Business	\$ 3,750,000	15%
Women Owned Small Business	\$ 2,250,000	9%

SECTION H – SPECIAL CONTRACT REQUIREMENTS

Service Disabled Veteran-Owned Small Business	\$ 1,750,000	7%
---	--------------	----

These goals will be assessed at the TO level as a percentage of subcontracted dollars.

In addition, the contractor shall execute a Subcontracting Plan which contains the contractor's efforts to meet the above small business subcontracting goals. If the contractor is a small business, the Subcontracting Plan is not required, and instead, the contractor shall provide Representations, Certifications, and Other Statements of Offerors.

As a part of the Subcontracting Plan, the contractor shall provide a Summary Subcontract Report (SSR) to the FEDSIM Basic Contract CO utilizing electronic Subcontracting Reporting System (eSRS) in Section J (Attachment P) no later than 30 days after the end of each contract year.

H.20 ON-RAMPING AND OFF-RAMPING

To ensure success of the USCYBERCOM Program, each contract holder is expected to participate in the ordering process by submitting proposals in response to RFPs for which the contractor has a reasonable chance for award, to successfully perform the terms of the orders, and to promptly improve performance when it does not meet the terms of the orders or the Basic Contract.

In addition, it is the Government's intent to maintain a qualified pool of contractors to ensure a reasonable expectation that each RFP competed under the contract meets the definition for adequate price competition. As such, if the contractor pool is diminished to a point where there is not an expectation that three or more responsible proposals will be received for a TO, the Government may hold an on-ramping season, thereby allowing offerors to compete for new Basic Contract awards. The contractor pool may be diminished over time through attrition, (e.g., industry consolidation without contract novation, industry consolidation by an existing USCYBERCOM Basic Contract holder, or other significant changes in the marketplace or advances in technology) by the Government exercising its rights under the terms and conditions of the contract or resultant TOs, or due to significant changes to the USCYBERCOM mission. The need to hold an on-ramping season will be at the Government's sole discretion.

H.20.1 ON-RAMPING PROCEDURES

If the CO determines that it would be in the Government's best interest to open a new solicitation to add new contractors to the USCYBERCOM Basic Contract, the CO may do so at any time provided that:

- a. The solicitation is issued under then-applicable Federal procurement law
- b. The solicitation identifies the total approximate number of new awards that the Government intends to make. The Government may decide to award more or fewer contracts than the number anticipated in the solicitation depending upon the overall quality of the offers received
- c. The award decision under any solicitation is based upon substantially the same evaluation factors/sub-factors as the original solicitation
- d. The terms and conditions of any resulting awards from a new solicitation are materially identical to the Basic Contract as modified

SECTION H – SPECIAL CONTRACT REQUIREMENTS

- e. The term for any such new awards from a solicitation is co-terminus with the existing term for all other USCYBERCOM contracts including the option period (if applicable)
- f. The award of any new Contract(s) does not increase the overall ceiling of the Basic Contract already awarded

H.20.2 OFF-RAMPING PROCEDURES

The CO reserves the unilateral right to Off-Ramp non-performing contractors. Contractors that are Off-Ramped have no active TOs under the USCYBERCOM Basic Contract at the time of the Off-Ramping.

Off-Ramping methods may result from one of the following conditions:

- a. Debarment, Suspension, or Ineligibility as defined in FAR Subpart 9.4
- b. Termination as defined in FAR Part 49
- c. Contractors who fail to meet the standards of performance, deliverables, or compliances
- d. Violation of security procedures
- e. Taking any other action which may be permitted under the USCYBERCOM Basic Contract terms and conditions

H.21 CROSS-TEAMING

- a. Basic Contract: Cross-teaming is a teaming arrangement in which prime offerors participate as a subcontractor/team member with another Prime or team member/subcontractor and/or subcontracts/teams with more than one prime contractor. Cross-Teaming is an arrangement between two Basic Contract Awardees. Prime/subcontractor relationships prior to Basic Contract award are not considered Cross-Teaming. An Offeror may, for example, compete to be the prime for one team and a subcontractor for another team. FAR 9.6 notes that Contractor team arrangements can benefit the Government by enhancing capabilities, performance, cost, and delivery factors. These arrangements can provide significant business benefits to the teaming partners, such as enhanced system and subsystem capabilities, a more substantial and relevant past performance record, and greater diversity. It is the Government's policy to recognize the integrity and validity of Contractor team arrangements and to not restrict the market provided, the arrangements are identified and company relationships are fully disclosed in an offer or, for arrangements entered into after submission of an offer, before the arrangement becomes effective. The Government will not normally require or encourage the dissolution of contractor team arrangements.
- b. Task Orders: The Government reserves the right to exclude prime contractor(s) from incorporating new cross teaming arrangements developed after award of the Basic Contract for the purpose of proposing on specific task orders. Each task order shall address whether or not crossing teaming will be allowed.

H.22 REQUESTING REMOVAL OF CONTRACTOR PERSONNEL

FEDSIM/USCYBERCOM retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this

SECTION H – SPECIAL CONTRACT REQUIREMENTS

contract, conflict with the interests of the Government. The reason for removal will be fully documented in writing by the CO. When and if such removal occurs, performance is acceptable when there is no mission impact due to position vacancies or unqualified personnel 100 percent of the time.

SECTION I – CONTRACT CLAUSES

I.1 TASK ORDER CLAUSES

In accordance with FAR 52.301, Solicitation Provisions and Contract Clauses (Matrix), the USCYBERCOM IDIQ master contracts cannot predetermine all the contract provisions/clauses for future individual task orders. However, all Applicable and Required provisions/clauses set forth in FAR 52.301 automatically flow down to all USCYBERCOM IDIQ task orders, based on their specific contract type (e.g. cost, fixed price etc), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the task order solicitation is issued.

However, the task order solicitation must identify whether FAR Part 12 commercial clauses/provisions apply or not apply. Furthermore, the Ordering Contracting Officer (OCO) must identify any Optional, and/or Agency-Specific provisions/clauses for each individual task order solicitation and subsequent award. For Optional and/or Agency-Specific provisions/clauses, the OCO must provide the provision/clause Number, Title, Date, and fill-in information (if any), as of the date the task order solicitation is issued.

I.2 USCYBERCOM BASIC CONTRACT CLAUSES

The following clauses apply to the USCYBERCOM Basic Contract and Seed TO 1 task order contract. The clauses, once incorporated into the basic contract, shall flow down to all other task orders under the basic contract unless otherwise stated. The clauses and dates remain unchanged throughout the term of the USCYBERCOM Basic Contract unless changed through a bi-lateral modification to the Basic Contract.

I.2.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: <http://www.acquisition.gov/far/>
<http://farsite.hill.af.mil>

I.2.2 GSAM 552.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (DEVIATION FAR 52.252-6) (SEP 1999)

(a) *Deviations to FAR clauses.*

(1) This solicitation or contract indicates any authorized deviation to a Federal Acquisition Regulation (48 CFR Chapter 1) clause by the addition of “(DEVIATION)” after the date of the clause, if the clause is not published in the General Services Administration Acquisition Regulation (48 CFR Chapter 5).

(2) This solicitation indicates any authorized deviation to a Federal Acquisition Regulation (FAR) clause that is published in the General Services Administration Acquisition Regulation by the addition of “(DEVIATION (FAR clause no.))” after the date of the clause.

(b) *Deviations to GSAR clauses.* This solicitation indicates any authorized deviation to a General Services Administration Acquisition Regulation clause by the addition of “(DEVIATION)” after the date of the clause.

SECTION I – CONTRACT CLAUSES

(c) “*Substantially the same as*” clauses. Changes in wording of clauses prescribed for use on a “substantially the same as” basis are not considered deviations.

(End of clause)

I.2.3 CLAUSES INCORPORATED BY REFERENCE - FEDERAL ACQUISITION REGULATION (FAR)

Clause No	Clause Title	Date
52.202-1	Definitions	(Jan 2012)
52.203-3	Gratuities	(Apr 1984)
52.203-5	Covenant Against Contingent Fees	(May 2014)
52.203-6	Restrictions on Subcontractor Sales to the Government	(SEP 2006)
52.203-7	Anti-Kickback Procedures	(May 2014)
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	(May 2014)
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	(May 2014)
52.203-12	Limitations on Payments to Influence Certain Federal Transactions	(Oct 2010)
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.203-14	Display of Hotline Posters (http://www.dodig.mil/Hotline/posters.cfm)	(Oct 2015)
52.203-16	Preventing Personal Conflicts of Interest	(Dec 2011)
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights.	(Apr 2014)
52.204-2	Security Requirements	(Aug 1996)
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	(May 2011)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204.10	Reporting Executive Compensation and First Tier Subcontract Awards	(Jul 2013)
52.204-13	System for Award Management Maintenance	(Jul 2013)
52.209-6	Protecting the Government’s Interest When Subcontracting with Contractor’s Debarred, Suspended, or Proposed for Debarment	(Aug 2013)
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	(Jul 2013)
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations.	(Dec 2014)
52.215-2	Audit and Records-Negotiations	(Oct 2010)
52.215-8	Order of Precedence—Uniform Contract Format	(Oct 1997)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.215-23	Limitations on Pass-Through Charges.	(Oct 2009)

SECTION I – CONTRACT CLAUSES

Clause No	Clause Title	Date
52.216-7	Allowable Cost and Payment.	(Jun 2013)
52.216-8	Fixed Fee	(Jun 2011)
52.219-8	Utilization of Small Business Concerns	(Oct 2014)
52.219-9	Small Business Subcontracting Plan	(Oct 2014)
52.219-14	Limitations on Subcontracting	(Nov 2011)
52.219-16	Liquidated Damages—Subcontracting Plan	(Jan 1999)
52.219-28	Post-Award Small Business Program Rerepresentation	(Jul 2013)
52.223-3	Convict Labor	(Jun 2003)
52.222-17	Nondisplacement of Qualified Workers	(May 2014)
52.222-21	Prohibition of Segregated Facilities	(Apr 2015)
52.222-24	Preaward On-site Equal Opportunity Compliance Evaluation.	(Feb 1999)
52.222-26	Equal Opportunity	(Apr 2015)
52.222-37	Employment Reports on Veterans.	(Jul 2014)
52.222-40	Notification of Employee Rights Under the National Labor Relations Act.	(Dec 2010)
52.222-41	Service Contract Labor Standards	(May 2014)
52.222-43	Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts).	(May 2014)
52.222-50	Combating Trafficking in Persons	(Mar 2015)
52.222-54	Employment Eligibility Verification	(Aug 2013)
52.223-6	Drug-Free Workplace	(May 2001)
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	(Aug 2011)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.225-13	Restrictions on certain Foreign Purchases	(Jun 2008)
52.227-1	Authorization and Consent	(Dec 2007)
52.227-13	Rights – Ownership by the Government	(Dec 2007)
52.228-7	Insurance-Liability to Third Persons	(Mar 1996)
52.230-2	Cost Accounting Standards	(May 2014)
52.230-6	Administration of Cost Accounting Standards	(Jun 2010)
52.232-17	Interest	(May 2014)
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-23	Assignment of Claims	(May 2014)
52.232-39	Unenforceability of Unauthorized Obligations	(Jun 2013)
52.232-33	Payment by Electronic Funds Transfer- System for Award Management.	(Jul 2013)

SECTION I – CONTRACT CLAUSES

Clause No	Clause Title	Date
52.232-40	Providing Accelerated Payments to Small Business Subcontractors.	(Dec 2013)
52.233-1	Disputes	(May 2014)
52.233-3 ALT I	Protest After Award– Alternate I (Jun 1985)	(Aug 1996) (June 1985)
52.233-4	Applicable Law of Breach of Contract Claim	(Oct 2004)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation.	(Apr 1984)
52.237-3	Continuity of Services	(Jan 1991)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.242-1	Notice of Intent to Disallow Costs	(Apr 1984)
52.242-3	Penalties for Unallowable Costs	(May 2014)
52.242-4	Certification of Final Indirect Costs	(Jan 1997)
52.242-13	Bankruptcy	(Jul 1995)
52.242-15 ALT I	Stop-Work Order- Alternate I (Apr 1984)	(Aug 1989) (Apr 1984)
52.243-2 ALT I	Changes – Cost Reimbursement Alternate I	(Apr 1984)
52.243-2 ALT II	Changes – Cost Reimbursement Alternate II	(Apr 1984)
52.243-2 ALT V	Changes – Cost Reimbursement Alternate V	(Apr 1984)
52.244-2	Subcontracts	(Oct 2010)
52.244-5	Competition in Subcontracting	(Dec 1996)
52.244-6	Subcontracts for Commercial Items	(Apr 2015)
52.245-1	Government Property	(Apr 2012)
52.245-9	Use and Charges	(Apr 2012)
52.246-25	Limitation of Liability – Services	(Feb 1997)
52.249-6	Termination (Cost Reimbursement)	(May 2004)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(Apr 2012)
52.253-1	Computer Generated Forms	(Jan 1991)

I.3 CLAUSES INCORPORATED BY REFERENCE - DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS)

The full text of a clause may be accessed electronically at:

DFARS website: <http://farsite.hill.af.mil>

Clause No	Clause Title	Date
252.201-7000	Contracting Officer's Representative	(DEC 1991)
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	(SEP 2013)
252.203-7003	Agency Office of the Inspector General	(DEC 2012)
252.203-7004	Display of Hotline Posters	(JAN 2015)
252.204-7000	Disclosure of Information	(AUG 2013)

SECTION I – CONTRACT CLAUSES

Clause No	Clause Title	Date
252.204-7003	Control of Government Personnel Work Product	(APR 1992)
252.204-7004	Alternate A, System for Award Management	(FEB 2014)
252.204-7005	Oral Attestation of Security Responsibilities	(NOV 2001)
252.204-7015	Disclosure of Information to Litigation Support Contractors	(FEB 2014)
252.209-7004	Subcontracting with Firms that are owned or controlled by The Government of a Terrorist Country	(MAR 2014)
252.211-7003	Item Identification and Valuation	(JUN 2013)
252.211-7007	Reporting of Government-Furnished Property	(AUG 2012)
252.215-7000	Pricing Adjustments	(DEC 2012)
252.216-7009	Allowability of Legal Costs Incurred in Connection With a Whistleblower Proceeding.	(SEP 2013)
252.223-7004	Drug-Free Work Force	(SEP 1988)
252.223-7006	Prohibition on Storage, Treatment, and Disposal of Toxic or Hazardous Materials	(SEP 2014)
252.227-7013	Rights in Technical Data - Noncommercial Items	(FEB 2014)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(MAR 2011)
252.227-7015	Technical Data-Commercial Items	(JUN 2013)
252.227-7016	Rights in Bid or Proposal Information	(JAN 2011)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(SEP 2011)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(JUN 1995)
252.227-7030	Technical Data- Withholding of Payment	(MAR 2000)
252.227-7037	Validation of Restrictive Markings on Technical Data	(JUN 2013)
252.231-7000	Supplemental Cost Principles	(DEC 1991)
252.232-7010	Levies on Contract Payment	(DEC 2006)
252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel	(JUN 2013)
252.239-7001	Information Assurance Contractor Training and Certification	(JAN 2008)
252.239-7010	Cloud Computing Services	(AUG 2015)
252.242-7005	Contractor Business Systems	(FEB 2012)
252.242-7006	Accounting System Administration	(FEB 2012)
252.244-7001	Contractor Purchasing System Administration	(MAY 2014)
252.245-7002	Tagging, Labeling, and Marking of Government-Furnished Property	(APR 2012)
252.245-7003	Contractor Property Management System Administration	(APR 2012)
252.245-7004	Reporting, Reutilization, and Disposal	(MAR 2015)
252.246-7001	Warranty of Data	(MAR 2014)
252.251-7000	Ordering From Government Supply Sources	(AUG 2012)

SECTION I – CONTRACT CLAUSES

I.4 CLAUSES INCORPORATED BY REFERENCE DEFENSE FEDERAL - GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM)

The full text of a clause may be accessed electronically at:

GSAM website: <http://farsite.hill.af.mil>

Clause No	Clause Title	Date
552.204-9	Personal Identity Verification Requirements	(Oct 2012)
552.215-70	Examination of Records by GSA	(Feb 1996)
552.216-74	Task-Order and Delivery-Order Ombudsman	(Aug 2010)
552.219-75	GSA Mentor-Protégé Program	(Sep 2009)
552.219-76	Mentor Requirements and Evaluation	(Mar 2012)
552.232-25	Prompt Payment	(Nov 2009)
552.236-75	Use of Premises	(Apr 1984)
552.237-71	Qualifications of Employees	(May 1989)
552.239-70	Information Technology Security Plan and Security Authorization	(Jun 2011)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

I.5 CLAUSES INCORPORATED BY FULL TEXT- (FAR)

52.216-19 Order Limitations (Oct 1995)

(a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than \$2,500, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order.* The Contractor is not obligated to honor --

(1) Any order for a single item in excess of \$300,000,000.00;

(2) Any order for a combination of items in excess of \$300,000,000.00; or

(3) A series of orders from the same ordering office within 15 days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (*i.e.*, includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 15 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

52.216-22 Indefinite Quantity (Oct 1995)

SECTION I – CONTRACT CLAUSES

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the “maximum.” The Government shall order at least the quantity of supplies or services designated in the Schedule as the “minimum.”

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor’s and Government’s rights and obligations with respect to that order to the same extent as if the order were completed during the contract’s effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 10 years and six months.

(End of Clause)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within anytime.

Special Contract Provision:

If the Government exercises its unilateral right to extend services under FAR 52.217-8, the unit prices for the performance of services during the extension period will be the unit prices contained in the contract for the last exercised period of performance.

(End of clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within anytime provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 5 calendar days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 Months.

(End of Clause)

SECTION I – CONTRACT CLAUSES

52.222-2 Payment for Overtime Premiums (Jul 1990)

(a) The use of overtime is authorized under this contract if the overtime premium does not exceed * _____ or the overtime premium is paid for work --

(1) Necessary to cope with emergencies such as those resulting from accidents, natural disasters, breakdowns of production equipment, or occasional production bottlenecks of a sporadic nature;

(2) By indirect-labor employees such as those performing duties in connection with administration, protection, transportation, maintenance, standby plant protection, operation of utilities, or accounting;

(3) To perform tests, industrial processes, laboratory procedures, loading or unloading of transportation conveyances, and operations in flight or afloat that are continuous in nature and cannot reasonably be interrupted or completed otherwise; or

(4) That will result in lower overall costs to the Government.

(b) Any request for estimated overtime premiums that exceeds the amount specified above shall include all estimated overtime for contract completion and shall --

(1) Identify the work unit; e.g., department or section in which the requested overtime will be used, together with present workload, staffing, and other data of the affected unit sufficient to permit the Contracting Officer to evaluate the necessity for the overtime;

(2) Demonstrate the effect that denial of the request will have on the contract delivery or performance schedule;

(3) Identify the extent to which approval of overtime would affect the performance or payments in connection with other Government contracts, together with identification of each affected contract; and

(4) Provide reasons why the required work cannot be performed by using multishift operations or by employing additional personnel.

* Insert either “zero” or the dollar amount agreed to during negotiations. The inserted figure does not apply to the exceptions in subparagraph (a)(1) through (a)(4) of the clause.

(End of Clause)

52.222-35 Equal Opportunity for Veterans (Jul 2014)

(a) *Definitions.* As used in this clause--

“Active duty wartime or campaign badge veteran,” “Armed Forces service medal veteran,” “disabled veteran,” “protected veteran,” “qualified disabled veteran,” and “recently separated veteran” have the meanings given at FAR 22.1301.

(b) *Equal opportunity clause.* The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) *Subcontracts.* The Contractor shall insert the terms of this clause in subcontracts of \$100,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor.

SECTION I – CONTRACT CLAUSES

The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate of identify properly the parties and their undertakings.

(End of Clause)

52.222-36 Equal Opportunity for Workers With Disabilities (Jul 2014)

(a) *Equal opportunity clause.* The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60.741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) *Subcontracts.* The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of \$15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of Clause)

I.6 CLAUSES INCORPORATED BY FULL TEXT- (DFARS)

252.203-7000 Requirements Relating to Compensation of Former DoD Officials (SEP 2011)

(a) *Definition.* “Covered DoD official,” as used in this clause, means an individual that—

(1) Leaves or left DoD service on or after January 28, 2008; and

(2)(i) Participated personally and substantially in an acquisition as defined in 41 U.S.C. 131 with a value in excess of \$10 million, and serves or served—

(A) In an Executive Schedule position under subchapter II of chapter 53 of Title 5, United States Code;

(B) In a position in the Senior Executive Service under subchapter VIII of chapter 53 of Title 5, United States Code; or

(C) In a general or flag officer position compensated at a rate of pay for grade O-7 or above under section 201 of Title 37, United States Code; or

(ii) Serves or served in DoD in one of the following positions: program manager, deputy program manager, procuring contracting officer, administrative contracting officer, source selection authority, member of the source selection evaluation board, or chief of a financial or technical evaluation team for a contract in an amount in excess of \$10 million.

(b) The Contractor shall not knowingly provide compensation to a covered DoD official within 2 years after the official leaves DoD service, without first determining that the official has sought and received, or has not received after 30 days of seeking, a written opinion from the

SECTION I – CONTRACT CLAUSES

appropriate DoD ethics counselor regarding the applicability of post-employment restrictions to the activities that the official is expected to undertake on behalf of the Contractor.

(c) Failure by the Contractor to comply with paragraph (b) of this clause may subject the Contractor to rescission of this contract, suspension, or debarment in accordance with 41 U.S.C. 2105(c).

(End of clause)

252.204-7009 Limitations on the Use of Third Party Contractor Reported Cyber Incident Information (AUG 2015)

(a) *Definitions.* As used in this clause—

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered defense information” means unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

SECTION I – CONTRACT CLAUSES

(b) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph

(b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items.

(End of clause)

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEVIATION 2016-O0001)(OCT 2015)

(a) Definitions. As used in this clause—

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

SECTION I – CONTRACT CLAUSES

“Contractor information system” means an information system belonging to, or operated by or for, the Contractor.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified information that—

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) Controlled technical information.

(B) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

“Cyber incident” means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

SECTION I – CONTRACT CLAUSES

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident. “Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

(A) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and

(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer with the exception of the derived security requirement 3.5.3 “Use of multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts”, which will be required not later than 9 months after award of the contract, if the Contractor notified the contracting officer in accordance with paragraph (c) of the provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (DEVIATION 2016-O0001)(OCT 2015); or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the DoD Chief Information Officer (CIO) prior to contract award; and

SECTION I – CONTRACT CLAUSES

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <http://dibnet.dod.mil>.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <http://dibnet.dod.mil>.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <http://iase.disa.mil/pki/eca/Pages/index.aspx>.

(d) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause. (h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark

SECTION I – CONTRACT CLAUSES

attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

- (1) To entities with missions that may be affected by such information;
- (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- (3) To Government entities that conduct counterintelligence or law enforcement investigations;
- (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
- (5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government’s use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts.* The Contractor shall—

- (1) Include the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and
- (2) Require subcontractors to rapidly report cyber incidents directly to DoD at <http://dibnet.dod.mil> and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next highest subcontractor) as soon as practicable.

SECTION I – CONTRACT CLAUSES

(End of clause)

252.216-7006 ORDERING (MAY 2011)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the contract schedule. Such orders may be issued from 1 June 2016 through 31 May 2021.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c)(1) If issued electronically, the order is considered “issued” when a copy has been posted to the Electronic Document Access system, and notice has been sent to the Contractor.

(2) If mailed or transmitted by facsimile, a delivery order or task order is considered “issued” when the Government deposits the order in the mail or transmits by facsimile. Mailing includes transmittal by U.S. mail or private delivery services.

(3) Orders may be issued orally only if authorized in the schedule.

(End of clause)

252.234-7002 EARNED VALUE MANAGEMENT SYSTEM (DEVIATION 2015-00017)(SEP 2015)

(a) Definitions. As used in this clause——

“Acceptable earned value management system” means an earned value management system that generally complies with system criteria in paragraph (b) of this clause.

“Earned value management system” means an earned value management system that complies with the earned value management system guidelines in the ANSI/EIA-748.

“Significant deficiency” means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b) System criteria. In the performance of this contract, the Contractor shall use——

(1) An Earned Value Management System (EVMS) that complies with the EVMS guidelines in the American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748); and

(2) Management procedures that provide for generation of timely, reliable, and verifiable information for the Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) required by the CPR and IMS data items of this contract.

(c) If this contract has a value of \$100 million or more, the Contractor shall use an EVMS that has been determined to be acceptable by the Cognizant Federal Agency (CFA). If, at the time of award, the Contractor’s EVMS has not been determined by the CFA to be in compliance with the EVMS guidelines as stated in paragraph (b)(1) of this clause, the Contractor shall apply its current system to the contract and shall take necessary actions to meet the milestones in the Contractor’s EVMS plan.

SECTION I – CONTRACT CLAUSES

(d) If this contract has a value of less than \$100 million, the Government will not make a formal determination that the Contractor's EVMS complies with the EVMS guidelines in ANSI/EIA-748 with respect to the contract. The use of the Contractor's EVMS for this contract does not imply a Government determination of the Contractor's compliance with the EVMS guidelines in ANSI/EIA-748 for application to future contracts. The Government will allow the use of a Contractor's EVMS that has been formally reviewed and determined by the CFA to be in compliance with the EVMS guidelines in ANSI/EIA-748.

(e) The Contractor shall submit notification of any proposed substantive changes to the EVMS procedures and the impact of those changes to the CFA. If this contract has a value of \$100 million or more, unless a waiver is granted by the CFA, any EVMS changes proposed by the Contractor require approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes as soon as practicable (generally within 30 calendar days) after receipt of the Contractor's notice of proposed changes. If the CFA waives the advance approval requirements, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Government will schedule integrated baseline reviews as early as practicable, and the review process will be conducted not later than 180 calendar days after—

(1) Contract award;

(2) The exercise of significant contract options; and

(3) The incorporation of major modifications. During such reviews, the Government and the Contractor will jointly assess the Contractor's baseline to be used for performance measurement to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

(g) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or duly authorized representative as necessary to permit Government surveillance to ensure that the EVMS complies, and continues to comply, with the performance criteria referenced in paragraph (b) of this clause.

(h) When indicated by contract performance, the Contractor shall submit a request for approval to initiate an over-target baseline or over-target schedule to the Contracting Officer. The request shall include a top-level projection of cost and/or schedule growth, a determination of whether or not performance variances will be retained, and a schedule of implementation for the rebaselining. The Government will acknowledge receipt of the request in a timely manner (generally within 30 calendar days).

(i) *Significant deficiencies.*

(1) The Contracting Officer will provide an initial determination to the Contractor, in writing, of any significant deficiencies. The initial determination will describe the deficiency in sufficient detail to allow the Contractor to understand the deficiency.

(2) The Contractor shall respond within 30 days to a written initial determination from the Contracting Officer that identifies significant deficiencies in the Contractor's EVMS. If the Contractor disagrees with the initial determination, the Contractor shall state, in writing, its rationale for disagreeing.

SECTION I – CONTRACT CLAUSES

(3) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer's final determination concerning—

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action;

(iii) System noncompliance, when the Contractor's existing EVMS fails to comply with the earned value management system guidelines in the ANSI/EIA-748; and

(iv) System disapproval, if initial EVMS validation is not successfully completed within the timeframe approved by the Contracting Officer, or if the Contracting Officer determines that the Contractor's earned value management system contains one or more significant deficiencies in high-risk guidelines in ANSI/EIA-748 standards (guidelines 1, 3, 6, 7, 8, 9, 10, 12, 16, 21, 23, 26, 27, 28, 30, or 32). When the Contracting Officer determines that the existing earned value management system contains one or more significant deficiencies in one or more of the remaining 16 guidelines in ANSI/EIA-748 standards, the Contracting Officer will use discretion to disapprove the system based on input received from functional specialists and the auditor.

(4) If the Contractor receives the Contracting Officer's final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the significant deficiencies.

(j) *Withholding payments.* If the Contracting Officer makes a final determination to disapprove the Contractor's EVMS, and the contract includes the clause at 252.242- 7005, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(k) With the exception of paragraphs (i) and (j) of this clause, the Contractor shall require its subcontractors to comply with EVMS requirements as follows:

(1) For subcontracts valued at \$100 million or more, the following subcontractors shall comply with the requirements of this clause:

[Contracting Officer to insert names of subcontractors (or subcontracted effort if subcontractors have not been selected) designated for application of the EVMS requirements of this clause.]

(2) For subcontracts valued at less than \$100 million, the following subcontractors shall comply with the requirements of this clause, excluding the requirements of paragraph (c) of this clause:

[Contracting Officer to insert names of subcontractors (or subcontracted effort if subcontractors have not been selected) designated for application of the EVMS requirements of this clause.]

(End of clause)

I.7 CLAUSES INCORPORATED BY FULL TEXT- (GSAMS)

552.232-78 COMMERCIAL SUPPLIER AGREEMENTS – UNENFORCEABLE CLAUSES (JULY 2015)

(a) When any supply or service acquired under this contract is subject to a commercial supplier agreement, the following language shall be deemed incorporated into the commercial supplier agreement. As used herein, "this agreement" means the commercial supplier agreement:

SECTION I – CONTRACT CLAUSES

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) Applicability. This agreement is part of a contract between the commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license (including all contracts, task orders, and delivery orders not using FAR Part 12).

(ii) End user. This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) Law and disputes. This agreement is governed by Federal law. (A) Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted. (B) Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted. (C) Any language prescribing different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.

(iv) Continued performance. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in 52.233-1 Disputes.

(v) Arbitration; equitable or injunctive relief. In the event of a claim or dispute arising under or relating to this agreement, (A) binding arbitration shall not be used unless specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).

(vi) Additional terms.

(A) This commercial supplier agreement may unilaterally incorporate additional terms by reference. Terms may be included by reference using electronic means (e.g., via web links, click and accept, etc). Such terms shall be enforceable only to the extent that:

(1) When included by reference using electronic means, the terms are readily available at referenced locations; and

(2) Terms do not materially change government obligations; and

(3) Terms do not increase government prices; and

(4) Terms do not decrease overall level of service; and

(5) Terms do not limit any other Government right addressed elsewhere in this contract.

(B) The order of precedence clause of this contract notwithstanding, any software license terms unilaterally revised subsequent to award that is inconsistent with any material term or provision of this contract is not enforceable against the government.

(vii) No automatic renewals. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term}, such license or service shall not renew automatically upon expiration of its current term without prior express Government approval.

SECTION I – CONTRACT CLAUSES

(viii) Indemnification. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(ix) Audits. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user's compliance with this agreement is hereby amended as follows:

(A) Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order.

(B) This charge, if disputed by the ordering activity, will be resolved through the Disputes clause at 52.233-1 ; no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process.

(C) Any audit requested by the contractor will be performed at the contractor's expense, without reimbursement by the Government.

(x) Taxes or surcharges. Any taxes or surcharges which the commercial supplier or licensor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract or order and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xi) Non-assignment. This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under the clause at 52.232-23, Assignment of Claims.

(xii) Confidential information. If this agreement includes a confidentiality clause, such clause is hereby amended to state that neither the agreement nor the Federal Supply Schedule price list shall be deemed "confidential information." Issues regarding release of "unit pricing" will be resolved consistent with the Freedom of Information Act. Notwithstanding anything in this agreement to the contrary, the Government may retain any confidential information as required by law, regulation or its internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this agreement.

(2) If any provision of this agreement conflicts or is inconsistent with the preceding subparagraph (a)(1), the provisions of subparagraph (a)(1) shall prevail to the extent of such inconsistency.)

End of Clause

I.8 DEPARTMENT OF HOMELAND SECURITY (DHS) ACQUISITION REGULATION SUPPLEMENTS (HSAR) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

SECTION I – CONTRACT CLAUSES

Clause No	Clause Title	Date
HSAR Class Deviation 15- 01	Safeguarding of Sensitive Information	(Mar 2015)

SECTION J – LIST OF ATTACHMENTS

J.1 LIST OF ATTACHMENTS

Attachment	Title
A	COR Appointment Letter (electronically attached .doc)
B	USCYBERCOM IDIQ Labor Categories and Definitions (electronically attached .pdf)
C	Problem Notification Report (electronically attached .pdf)
D	Corporate NDA Statement (electronically attached .pdf)
E	Removed at Award
F	Removed at Award
G	Removed at Award
H	Quality Assurance Surveillance Plan (electronically attached .pdf)
I	Removed at Award
J	Removed at Award
K	Acronym List (electronically attached .doc)
L	Removed at Award
M	Removed at Award
N	Removed at Award
O	Removed at Award
P	Electronic Summary Subcontract Report Instructions (electronically attached .pdf)
Q	Current Environment at Award (electronically attached .pdf)
R	USCYBERCOM and NSA Non-Disclosure Agreements for Contractor Employees (electronically attached .pdf)
S	Removed at Award

